Global Information Assurance Certification Paper

This paper is related to GSEC Version 1.4b - option 2.

I-VPN Porting a corporate network to Internet

Thorstein Oeverby
March 25. 2003

Abstract

This paper describes the process of implementing a corporate business network over Internet that replaces a variety of communication solutions developed over the years.

My company is a chemical company with plants and offices spread worldwide. Most of our IT-systems are run centrally at the head quarter with a combination of online solutions and database replication for the branch offices. Prior to this project, we had several communication solutions implemented for the systems. The ERP system was carried over Frame Relay connections and other systems was set up with different dial-up solutions and - to some degree - leased lines. The variety of solutions was difficult to maintain, and the total cost was high and quite difficult to follow up. We also noticed emerging needs for general use of Internet by our users. On these bases, we initiated a project with the mandate of a total redesign and renewal of our communication solutions.

The paper addresses the security aspects and other major elements that were focused on during the process of choosing the solution best suited for my company. The situation before and after the project is described, as well as the basis and possible options that lead to the decisions we had to make along the way. Details about the implementation of the solution are also covered, and the lesson learned in the process is discussed. Finally, the cost-benefit aspect of the project is examined, and our conclusion that this was a successful project is substantiated.

Background

The ERP-system of our business was due for an upgrade. This was the direct cause to change our current communication solutions. The solutions were working, but the ERP-upgrade required more bandwidth and our F/R-connections were expensive to upgrade. Our other communication solutions also showed high cost and were difficult to maintain, due to lack of standardization.
The F/R-connection for the company headquarter (hereafter referred to as "the IT-Center") was secured and controlled through our CheckPoint firewall, as well as the Internet access.
This connection was basically used for SMTP-mail, browsing and downloading. Internet access for our users were controlled and based on business needs.
Users at the branch-offices also had needs for browsing, downloading and other Internet based applications. Most sites had several PC's with a dial-up Internet connection for such use. These PC's were usually not secured in any matter although some of them also were LAN-connected. Thus they represented a security hazard to our network.

Given these premises, we decided to look for other options based on up-to-date technology. I was given the task "come up with a more secure and cost effective way of communication between our sites".

We wanted a backbone network that could carry basically all types of IT-communication with focus on:

- Cost efficiency (optimal price/performance)
- Security
- Availability
- Performance and scalability
- Solutions based on standards and market leading products

The project was initiated with the writer as the only participant, reporting to the IT-manager. As the project developed and materialized, an experienced security professional from our chosen partner joined in. My own role through the project was research, evaluating the options with recommendation for decision making and total project management. Based on my background as a networking engineer, I sorted out the options and basis for the numerous decisions, and presented the material for the IT-manager with recommendations. These were on the whole followed, and the financing was put in place after a cost / benefit evaluation.

Preliminary check

Sources on the Internet, and a check with different communication providers and other companies with similar IT-structure, pointed all in the direction of Internet for all needs.

Reference [1]

> *"The Internet is critical to business. Companies have no choice but to connect their internal networks to the rest of the world - to link with customers, suppliers, partners, and their own employees. But with that connection comes new threats: malicious hackers, criminals, industrial spies.*
> *…. As risky as the Internet is, companies have no choice but to be there. The lures of new markets, new customers, new revenue sources, and new business models are just so great that companies will flock to the Internet regardless of the risks. There is no alternative. This, more than anything else, is why computer security is so important."*

There were many good reasons for using the Internet for information transport, also for business critical information. Internet was coming available almost everywhere, normally to a reasonable cost, with a tendency of improving cost/benefit.
The scalability was no problem since the access can be bought at almost any speed rate and the backbone capacity is huge. Stability was also improving, so all in all, most communication providers marketed Internet as the preferable carrier for most types of IT-communication.

The major advantage for Internet over the other options, was cost, availability and scalability. Low cost is often the major element initially and by far the easiest way to

get an acceptance by the management, but unstable solutions are not appreciated and will quickly cause dissatisfied users and trouble.

The major concern for using the Internet for business critical information was the security aspect. Information is subjected to possible misuse, that can be both stealing and manipulation. Internet is an insecure place, with - at best - diffuse ownership and responsibilities. Corporations must be able to protect their confidential data from misuse as it travels through a global network.
Solutions for safe and reliable communication over Internet were now available, and had been on the market for some time.

The second concern was related to stability. Porting our business critical applications to Internet would make us very vulnerable for disturbance of any kind on the net. Our own experience with Internet over the last years was that the stability was improving, but still was somewhat worse than desired. But, then again, the other communication options were not 100% stable either.
We had also heard of DoS attacks and the possibility of being totally blocked out from Internet.

These issues were addressed in a small project with participants from potential communication providers. After discussing the pros and cons with different solutions, following up the objections and checking other companies' experiences, we concluded that using Internet for all needs was the way to go, provided that the right technology was implemented.

The communication industry and the IETF (Internet Engineering Task Force) had worked for years on good and reliable security solutions for Internet use. Now, after lots of trial and adjustments, a solution based on IPSec materialized as a standard. The standard was named VPN (Virtual Private Network).

Reference [2]

> Translated from Norwegian:
> *"VPN is easiest described as a tunnel through existing infrastructure - a virtual connection between two points. The walls of the tunnel are secured by encryption technology, so the data transmitted is - if not invisible, so at least unreadable for outsiders."*

VPN is a collective term for techniques giving safe transport of information over unsecured communication channels, such as Internet. Several techniques was used for establishing a VPN, but the combination of the tunneling protocol L2TP and the architecture of IPSec seemed to be a winning combination in the market.

VPN functionality is installed in both ends of the communication lines - often parallel to or inside the firewall function for the business sites, creating a protected "tunnel", a peer to peer solution, experienced as a private network. VPN incorporates authentication of users and sites and encryption of data, and was considered as safe and unbreakable. Several multinational companies had already been using the technique for some time, so it was well proven.
VPN used over Internet is often referred to as I-VPN.

Goals

The goals of the project - named I-VPN was specified to:

Creating a worldwide company backbone network over Internet, capable of carrying basically all types of IT-communication.

The network should cover all permanent site to site communication between 12 defined sites, with a possible extension to more sites and solutions for Home Office and mobile users.

Risk analysis and threat evaluation

None of our IT-systems were regarded as a "sensitive system" with special regulations by law, so it was our own decisions how we would exploit the Internet. The risks of communicating over Internet were presented for the corporate management, which had no objections to proceed given adequate design, protecting mechanisms and routines for monitoring and control. Though we had not implemented specific procedures related to the security standard BS 7799, we had it in mind designing our solutions.

First we performed a risk analysis regarding confidentiality, integrity and availability.

Our research led us to the conclusion that the IPSec encrypting function handled the confidentiality. A variety of encryption algorithms were available with 3DES as the best option at the time. 3DES was considered safe and unbreakable, so we chose that with encryption keys set up to change every 60 minutes.

Regarding integrity, there were already in place procedures for physical access and user authentication, giving us quite good control of the connected users. Integrity between the sites was also vital, and could be handled in various ways, for instance shared secrets in the firewalls.

Availability was another matter. We wanted as close to 100 % (24 x 7) uptime as possible for the IT-Center, but could allow some downtime for the branch offices since their normal use took place during office hours. We would consider a backup solution over another media than Internet to prevent too much downtime in case of for example disruption of the local access.
The emerging DoS-problem could be a threat for the availability, so this was given special attendance at a later state in the project.

Defense in depth

We want to build the security in several layers, and segmenting the traffic will contribute to better total security. We decided that all WAN access to our LAN's should be routed over the firewalls. No direct external access to internal services. All types of access from Internet should go through services on separate segments connected to our firewall - so called DMZ zones.

Reference [3]

> *"A DMZ is a glowing example of the Defense-in-Depth principle. The Defense-in-Depth principle states that no one thing, no two things, will ever provide total security. It states that the only way for a system to be reasonably secured is to consider every aspect of the systems existence and secure them all. A DMZ is a step towards defense in depth because it adds an extra layer of security beyond that of a single perimeter."*

Servers with services available to the Internet shall not have general access to internal resources. Communication to these servers from the LAN-servers should always be initiated from the inside, and with different technology than the service open to Internet.
This is also compliant to the strategy "Defense in depth", which we try to implement on all levels of our systems.

Mandate needed

We wanted to implement a common communication security policy for the whole network, and for this we needed an extended mandate. Prior to this project, the IT-Center had limited responsibilities for the IT-solutions for the branch offices other than providing access to the servers running the ERP-system and the E-mail.

A common Internet Policy was worked out, and routines for implementation and use were established. Implementation, setting of security rules, distribution of security keys, facility management and monitoring for the entire corporate backbone network will be lead and coordinated by the IT-Center.

Responsibility

Our major concern - security, could be handled in several ways. We could set out the VPN function to a network provider as a delivered service (later called PPVPN *[Reference [4]*), or we could handle the VPN ourselves.
The responsibility for the security however, can not be outsourced.

Some of the world wide ISP's offered a managed VPN service, but the product was at the time quite new and not yet "settled", and the cost was relatively high compared to VPN in own stage management. The VPN-solutions delivered by the ISP's were at the time quite different and minor ISP's did not offer the function at all.

We decided to manage the VPN-function ourselves. Full control of the security aspect was the major reason for this choice, but it also would give us a total flexibility in choice of carriers. All we needed from an ISP was a good and stable connection - no extra functionality. Being so flexible regarding carrier, we would be able to get the best price / performance at any time. Even though price / performance regarding communication is improving, this is not automatically achieved. Being able to change ISP without too much fuzz is a good base for cost optimization.

Technical Solution

There were numerous vendors on the market with VPN-products. Some vendors with VPN incorporated in firewalls, and some with dedicated VPN-solutions in specialized hardware. My company had been using FireWall-1 from CheckPoint as firewall function for several years. FW-1 was market leader in firewall products, and their recent focus on VPN called VPN-1 had the functionality we wanted. FW-1 also had mechanisms for special handling of SYN attacks, reducing at least this DoS threat. Our final choice - continuing with CheckPoint and implementing VPN in the firewalls- was based on the following:

- Our focus regarding solutions based on standards and market leading products
- Previous good experience with CheckPoint's FW-1
- We already had some in-house competence on FW-1
- Good access to external competence for FW-1
- CheckPoint's technology that combined firewall- and VPN functionality

We believe in building upon previous installations (if our experiences with it are positive) to get more out of our investments in competence, time and money. Other options are always considered regarding function and cost, but if no major disadvantages are found, an extension of an existing system is often preferred.

Having decided on a VPN-solution over Internet, based on CheckPoint's VPN-1 technology and obtained the mandate to implement the solution for the sites involved, there still were many things to consider and decisions to make.
These were:

- Determine bandwidth needed and grade of redundancy
- Choice of ISP(s)
- Choice of firewall platform
- Obtain necessary competence for setup and maintenance of the firewalls and VPN

We also designed and implemented an ISDN-based backup solution for emergency use, in case of enduring downtime of the I-VPN solution.
The solution cover only defined business critical applications.
In all, I-VPN in combination with the ISDN-backup gives us a total solution that is more reliable and robust, and the result is higher total availability.

Bandwidth

Previously we had decided to use "Thin Client" technology and the Citrix ICA solution for access to our central IT-systems. Using the thin client concept has also a security benefit, since all data is stored on the central servers.

Reference [5]

> *"ICA is optimized for connections as low as 14,4 Kb/s. Only mouse clicks, keystrokes and screen updates travel the network to generate exceptional performance. On the client, users see and work with the application's*

interface, but 100 percent of the application executes on the server. And with ICA, applications consume as little as one-tenth of their normal network bandwidth."

Testing the ICA-client, we found that the figures from Citrix were quite accurate. Taking into account that 128 Kb/s was needed as a minimum level for good VPN-function, we ended up with 128 Kb/s for most sites, and 256 Kb/s for a couple of sites with more users.
128 Kb/s and 256 Kb/s were not available at some sites, so the next "step" available was decided for these sites.

Having permanent Internet accesses for each site, we wanted to open up for browsing, downloading and other suitable Internet based applications as an add-on for the branch offices. This would make their dial-up Internet solutions obsolete, which would result in enhanced security as well as reduced costs and an upside to the project.
However, extensive WEB browsing can easily "eat up" all available bandwidth. This was an issue that required caution. Internet bandwidth is still quite expensive - at least dealing with global carriers. Obtaining control here requires either implementation of special software or at least (for small environments) a manual control established by means of caution and good information. To ensure good function for our business critical applications, opening for WEB browsing was postponed until we were sure that the solution was running stable, and available bandwidth was sufficient.

Choosing ISP

Internet access has become available on several techniques, and the providers are numerous. Checking the options, we were offered 128 Kb/s access to our branch offices with costs from US$ 50 to US$ 8.000, with lots of options in between! What was the difference between these offers, and what should we choose? Should we go for one global carrier for all sites, or pick a local ISP based on cost and service?

A sectional project was set up with the mandate of choosing the ISP for this VPN-project. Since we had decided to manage the VPN-function ourselves, our criteria for choice of ISP were presence, stability, latency and cost.
Our Thin Client solution is quite latency sensitive, and only the global ISP's could offer latency guaranties between our sites, so we decided to go for a global ISP. This excluded the cheapest options, normally offered by local vendors.
Checking the products and offers of the numerous ISP's were quite time-consuming, so this part of the project took a couple of months. Having made our choice and ordered the connections, the installation took more than 3 months.

Firewall platform

Previously we had run the CheckPoint firewall on a HP-Unix platform. Available options were several: Solaris, Linux, Windows NT, IPSO and more.

Evaluating the options, we finally went for the IPSO-solution, now handled by Nokia, delivered on specialized hardware and hardened for firewall use.

In my opinion, a specialized OS, security hardened for the task is preferable for such a vital function as a firewall. I often heard the phrase "the security offered by the firewall is not better than the security implemented in the OS". This makes sense to me, and became an issue in the decision. Specialized hardware has both positive and negative aspects, but the products delivered by Nokia were well suited for our needs. Their worldwide service option was also suited for our corporation.

Skills development

Our CheckPoint firewall had been in operation for a while, but we had problems maintaining good function and adequate security. Our skills regarding management of the firewall were also somewhat out of date and needed upgrading as well as our routines regarding log checking and follow up of incidents.
Despite having some in-house competence on the product FW-1, we soon realized that we had a serious upgrade to do to cope with the general development for the product and VPN-function. The options were:

- Take the time and resources to build necessary skills for own personnel.
- Hire trained personnel.
- Find a competent partner for facility management of our own equipment.
- Full outsourcing of the solution.

Given restrictions from our management regarding own personnel, and our policy of controlling the security ourselves, we decided to find a suitable partner that could guide us through the implementation of the project. We also wanted this partner to do the installation and setup of the total solution including delivery of hardware and do facility management of the total solution afterwards.
3 potential partners were evaluated and we made our choice based on the delivered offers, ability to accommodate to our needs and a general impression of the partner.

Implementation

The project was divided in 2 phases:

Phase 1: Upgrade of the security system at the IT-Center

- Installation of a central management server.
- Installation of a "High Availability" firewall solution with NIC's for 8 segments.
- Redundant switches for the external firewall segments.
- Installation of an ISDN-router for the backup solution.
- Upgrade of Internet access. A 2 Mb/s main access delivered on fiberoptical connections and a 1 Mb/s backup access delivered on traditional copper lines.

Redundant access delivered over completely different infrastructure and separate routers should result in a more stable access. The two lines were also connected to different access points on the ISP side.

Phase 2: Rollout at the external sites

- Single Internet access (bandwidth 128 Kb/s or more).
- A Nokia IP 110 firewall with IPSO software, CheckPoint FW-1 inspection module and VPN functionality.
- An ISDN-line and a router for the backup solution.

Phase 1 was a quite big upgrade and a total reinstallation of our existing firewall installation. We installed a separate administration server capable of administration and logging of traffic from all firewalls. A new version of CheckPoint FW-1 was installed, and the existing rules were critically checked and refreshed. Two new Nokia IP 440 firewalls with IPSO OS were installed in a fail-over cluster, upgraded with software for VPN and 3-DES encryption.

All external segments were set up with separate redundant switches.
After this installation was tested and proven stable for the existing services, we proceeded with the next phase.

Phase 2 involved several elements of coordination: Deliverance of access line and router from the chosen worldwide ISP, firewall and ISDN-router setup and shipment done by our partner, installation, test and adjustments in co-operation with our local IT-person.
Some of the sites had a function dedicated to the IT-systems, part-time or full time, but some sites were so small that this LSA-function (local system administrator) was not defined. Having no skilled IT-person on site is quite a challenge, since basic functions for the local PC's and servers are also impacted. Physical installation, DNS-setup, IP-configuration, default gateway and so on had to be changed. Most sites were able to obtain local skilled help, so we managed.

Routines for fault checking, monitoring and reporting were worked out and responsibilities for the different elements in the new solutions were put in place.

Prior to connecting the Internet access, we checked all sites for PC's connected to the LAN with dial-up solutions to Internet. These PC's were first disconnected from the LAN, and at a later state made obsolete by opening for controlled browsing through the firewall.

PC's at the external site that should be used for the central ERP-system were set up with a Citrix ICA client, and necessary definitions for authentication and authorization were made.

The sites were set up one by one, with few unforeseen problems. After disconnecting the F/R-router and connecting the new WAN-router with the firewall, establishing the VPN connections was quite straightforward though rather manual work. This was the task of our partner, and they showed their competence, having the solutions up and running stable in a matter of hours.

Costs

In total we invested about US $ 200.000 on this project.
Of this relates US $ 80.000 to investments at the IT-Center and US $ 120.000 as a total for all branch offices.

The maintenance cost savings after the project consist of lower communication cost due to use of Internet, which is much cheaper than the F/R-option. Maintenance and monitoring of the security functions though, is an extra cost, but in total we have a good gain compared to the situation before the I-VPN project.
We estimate reduced costs in the amount of US $ 16.000 pr. month, giving a payback of the invested money of a little more than one year.
Estimated yearly savings: roughly US $ 190.000.

Findings and lesson learned

As mentioned, parallel to changing the communication solution, we also implemented the concept of thin clients - running the Citrix ICA protocol for low bandwidth usage. This introduced an extra level in the total solution in addition to the firewalls and VPN. The security implemented by VPN has proven to be stable, quite manageable and - hopefully - adequate. We are quite pleased with our partner that does facility management of the solution, and we feel that the routines put in place for maintenance and follow up of the security is functioning well.

Our main concern regarding latency and the Citrix ICA solution was real, and we had to do some adjustments of the client and implementation of a simple mechanism for prioritization of the ICA protocol. After this, in normal operation, the users did not feel any noticeable difference compared to running the old version of the ERP-system with native clients over F/R, and they were quite satisfied with the functionality.

The downside of the solution is that troubleshooting and correction has become more complex. We have had a few problems with the firewalls due to both hardware trouble and setup errors. These problems have been quite easy to define and correct, but we have also experienced unstable network performance, which is much harder to correct and even get acceptance for by the ISP.
For the end users it works or it does not work, if the problem is at the local PC or network, in the firewall or VPN, Internet performance, WTS-servers or at the ERP-system is not always obvious. The fact that there are long distances and different time zones between the users and the IT-Center does not make things easier. This is a big challenge for our support function.
On some occasions, we have had poor network function resulting in slow performance and dropouts for the users. Complaining to our ISP, they informed us that for at least one of these trouble periods they had experienced a massive DoS attack to one or several customers on their network. This impacted the overall performance of most customers in the same region for a period of several hours.

Extension of the solution

The basic investments for a total I-VPN network for the whole business are in place after this project. Extensions are quite easy and will have relative low costs, since the structure and central functions already are in place.
The VPN technique has potential far beyond the scope of this project, and can be used also for communication to partners and customers. CheckPoint's product series also include software-based solutions suitable for SOHO (Small Office Home Office) and mobile users. The product - called VPN-1 SecureClient is designed for use in an environment with CheckPoint firewalls.

Reference [6].

> *"For network administrators who currently use Check Point's FireWall-1 solution for their firewall and want to extend VPN access to a large number of users – SecureClient is a clear choice. It protects those computers outside the corporate firewall while allowing them complete access to all necessary applications through industry standard VPN tunneling techniques. It also integrates seamlessly with the existing infrastructure, updates automatically, and has other features designed to add flexibility and usability to the product."*

We have also implemented these solutions, for external consultants working remote on our solutions, for some one-man's sales offices, and also for more than 200 Home offices and Nomads.
The SecureClient solution is very functional giving us extra value for our investments in the I-VPN project, though the PC-installations and the numerous different Internet connection types has given us quite much trouble. We have users accessing the IT-Center and their local branch office as well as the open Internet seamlessly.

Conclusions

Regarding security, we feel that our solution is adequate. Normally, security impacts functionality, but in this case we have been able to implement good security and still has a user-friendly solution.
The routines we implemented regarding monitoring and control of events is functioning well, giving us a certain view of threats and events.
We are worried by DoS attacks, but have so far not addressed this further.

In the IT-business things change fast, so when you decide on a solution, you must always be ready to revalue your decisions and make necessary changes. It seems that what we implemented in our I-VPN project is becoming common in the business, and this is often a good sign that your own choices were the right ones.
The products used in the network are showing reduced cost, so the cost / benefit for the solution is also improving for extension of the project.

All in all both the users, the company management and the IT-professionals are satisfied with the project, so we regard it as a successful project.

References

[1]
From Managed Security for the 21st Century by Bruce Schneier
http://www.counterpane.com/msm.pdf
[2]
"Network architecture for the 21st Century".
Special report from Team Mellvik AS (ISBN 82-91519-07-2)
http://www.mellvik.no/MR/index.html
[3]
SANS top-paper "Designing a DMZ" by Scott Young March 2001
http://www.sans.org/rr/toppapers/DMZ.php
[4]
IETF working group on PPVPN
http://www.ietf.org/html.charters/ppvpn-charter.html
[5]
Citrix Independent Computing Architecture (ICA)
http://www.citrix.com/site/PS/products/feature.asp?familyID=19&productID=1449&featureID=3955
[6]
SANS Reading Room "VPN-1 SecureClient - CheckPoint's Solution for Secure Intranet Extension" by Ryan Gibbons April 2002
http://www.sans.org/rr/encryption/secureclient.php