RAPPORT DE STAGE

Christophe LE ROQUAIS, Elève ingénieur 5ème année
Département Télécommunications, Services&Usages

Stage effectué au sein de TOTAL FINA ELF
33, Cavendish Square LONDON
du 02 septembre 2002 au 17 janvier 2003

RAPPORT DE STAGE

Christophe LE ROQUAIS, Elève ingénieur 5ème année
Département Télécommunications, Services&Usages

Stage effectué au sein de TOTAL FINA ELF
33, Cavendish Square LONDON
du 02 septembre 2002 au 17 janvier 2003

SUMMARY

TotalFinaElf is one of the biggest oil companies in the world. The London site is specialised in the Gas and Electricity trading. The IT needs are very important. I was a member of the IT staff that comprises of ten people whose Philippe Guelminger who is the Manager. Thanks to his managerial abilities, the work accomplished by the team is outstanding: efficiency in a pleasant atmosphere.

During this training-period, I was in charge of three main projects, all of them related to network security. I first focused on the designing and the implementation of a VPN security platform. My second project was to design and to implement a solution to analyse the firewall logs. Last, I was responsible for specifying and supervising a project to integrate a network for securing remotely the client workstations.

RESUME

TotalFinaElf est un des groupes pétroliers les plus importants au monde. Le site de Londres est spécialisé dans le trading gaz et électricité. Les besoins en informatique, réseaux et télécoms sont très importants. J'ai fait partie de l'équipe informatique qui comprend dix personnes dont Philippe Guelminger, le manager. Grâce a ses capacités manageriales, le travail réalisé par l'équipe est remarquable : efficacité dans une bonne ambiance.

Trois projets principaux m'ont été confiés pendant ce stage, tous en relation avec la sécurité des réseaux. J'ai d'abord été charge de l'étude fonctionnelle et technique d'une plate forme sécurité VPN. Le second projet a été de concevoir et de mettre en place une solution d'analyse des logs de sécurité au niveau des firewalls. Enfin, j'ai été responsable des spécifications et du suivi d'un projet d'intégration de réseau pour la sécurisation a distance des postes clients.

CONTENTS TABLE

Introduction

The TotalFinaElf site in London belongs to TFE Gas&Power (TotalFinaElf branch). The core activity is Gas and Electricity trading.

I was employed as a member of the IT team that comprises of ten staff. Their goal is to maintain and to enhance the network, the databases, the telecommunications and everything relating to IT generally. Due to the core activity business, the IT/networks are very numerous and are often critical devices.

I wanted to find a training-period abroad as I had already carried out two training-periods in France before and I wanted to get hands on experience overseas. I can say this training-period in London was very worthwhile. I found this training-period by finding an old TFE training-period offer on the Intranet of the department. I decided to contact Michel Guillé, Gas&Power IT Director, to ask him if there were training possibilities in London. He answered me quickly and he proposed we meet together in London.

In May 2002, I met Michel Guillé and Philippe Guelminger (London IT Manager). Our meeting was a quick presentation to talk about the training subject and about the conditions of the training-period.

1. PRESENTATION OF THE COMPANY

1.1. TotalFinaElf

TotalFinaElf is one of the leading oil companies in the world. With operations in more than 100 countries, the Group's activities span all aspects of the energy industry from Upstream to Downstream.

- **Upstream**: oil and gas exploration and production
- **Downstream**: refining and marketing of refined products as well as international trading in both crude and refined products.

Fig. 1: TFE headquarters in Paris

TotalFinaElf is also a major player in the Chemicals markets.

Boasting, one of the fastest growing and most geographically diverse portfolios of oil and gas properties in the industry, TotalFinaElf currently produces more than 2 million barrels of oil equivalent per day from proved reserves of more than 10 billion barrels.

The Group is a leading player on the European refining and marketing scene, having an interest in 29 refineries and operating a network of about 20,000 service stations concentrated primarily in Europe and Africa, TotalFinaElf's Chemicals activities include a petrochemicals segment, typically associated with major integrated oil companies.

As well as a specialty chemicals segment focusing on industrial rubber processing and a range, of coatings including parties, resins, adhesives and electroplating.
Combining the strengths of Total, PetroFina and Elf Aquitaine, the new Group is well positioned to ensure future growth and take its place as one of the largest and most competitive players of the industry.

In the Upstream, by the end of year 1999, TotalFinaElf's hydrocarbon reserves rose to 10.5 billion barrels of oil equivalent, representing nearly 14 years of production at the current rate of 2.1 million barrels per day.

The Group has delivered rapid growth in terms of both production and new reserve additions and with TotalFinaElf's participation for major projects with low technical costs - particularly on some very promising deep-offshore permits - the stage is set for further steady growth. The Group's asset portfolio is well balanced between the OECD zone anti emerging countries.

The three main production zones are the North Sea, Africa and the Middle East, with remaining Output shared between the Americas and Southeast Asia.

About two-thirds of the Group's production is liquids, oil and condensates, and the remaining one-third is gas. Worldwide demand for natural gas is growing more rapidly than the demand for oil. TotalFinaElf is well positioned as one of the top world producers of liquefied natural gas (LNG) and is rapidly expanding its gas activities in the Far East, the Middle East, Latin America and Europe with an eye towards developing new market segments, including gas supply and power generation.

In the downstream, TotalfinaElf has a refining capacity of about 2.6 million barrels per day from a network of efficient, well-located refineries. Considerable progress has already been made for bringing break-even points down to very low levels. TotalFinaElf expects that future synergies linked to the two successive mergers will enable it to continue to improve competitiveness.

In Marketing, the Group's refined product sales, excluding trading, averaged 3.2 million barrels per day in 1999. With its marketing policy focused on product anti service quality, TotalFinaElf is now the leading oil-product marketer for France and the Benelux countries.

In Europe, the group is the leader in retail distribution with an average of 12% of the market share through its network. Outside Europe, TotalFinaElf is focusing on high-growth zones such as Africa (where the Group is the leading marketer continent-wide), the Mediterranean Basin and Southeast Asia, and on specialty products, such as heating fuels, liquefied petroleum gas, aviation fuel, lubricants, waxes, bitumens and solvents.

In Chemicals the Group's activities includes petrochemicals & plastics, intermediates & performance polymers as well as specialty chemicals. Atofina is a European and worldwide leader in each of these market segments. The group's petrochemicals units, which will now benefit front closer integration with refining operations, are concentrated primarily in low-cost facilities in Europe and the United States, positioning the company as a major global supplier of intermediates and plastics. Atofina is the world's second-largest producer of polypropylene, and is the fourth-largest supplier of polyethylene and the third-largest producer of polystyrene in Europe.

The Group is also a major world player in a number of intermediate chemicals, ranking as the largest producer of thiochemicals, second-largest supplier of fluorochemicals, and third-largest in acrylics and peroxides.

In the specialty chemicals segment, TotalFinaElf focuses on high-tech rubber processing (the Group Subsidiary Hutchinson is the second-largest industrial rubber products producer in Europe) and on coatings such as paints (SigmaKalon is the second-largest decorative paints producer in Europe), resins (TotalFinaElf second-largest producer of resins in the world via Gray Valley in Europe and Sartomer and Cook Composites in the United States), and adhesives (the Group is second-largest producer worldwide with Bostik and Ato Findley).

1.2. TotalFinaElf Gas&Power

TotalFinaElf Gas&Power is the Gas and Electricity branch. It is composed of four activity poles: Strategy Finance Other Energies, Business Development, Trading&Marketing, General Administration.

The gas and power business in the UK is part of Trading Gas and Electricity within the Exploration and Production division of the group. It operates in the UK, Europe and the US with offices in London, Paris, Brussels and Houston. It is one of the largest gas, electricity and derivatives traders in Europe. TotalFinaElf Gas and Power provides access to the traded markets for all the Group's gas that is not committed to long term contracts and supplies gas to the marketing businesses. It is also responsible for the development of European business that is linked to traded markets. It operates 40% of Humber Power, representing about 500 megawatts and trades the electricity produced into the UK market. Within the UK, TotalFinaElf Gas and Power has 11 per cent of the industrial and commercial markets. This represents over a billion terms a year and 40,000 customers. The sales operation employs approximately 150 people based in Redhill, south of London. The Corporate Services and Risk Management of gas, electricity and LNG trading and marketing are based at Cavendish Square where approximately 100 people are employed. The combined turnover, including trading amounts to £3.2bn.

1.3. The IT Staff

During my training-period, I was a member of the IT staff. The team work was very important, each position being complementary to others. The work atmosphere was really good and I thank all the staff for their kindness. The IT staff is composed of:

Philippe GUELMINGER, IT Manager
Cedric DENECE, Network Security and Infrastructure manager
Gérôme BILLOIS, Network and Infrastructure Controller
Simon AMBROSE, Database Administrator
Chris SYMEON, IT Support Manager
Keith GATT, Network Controller
Véronique EVARISTE, Webmaster and Lotus Notes Designer
Wayne WILLIAMS, Telecommunication engineer
Clement HARRY, IT Technician
Emile HANSON, IT Technician

2. MAN MANAGEMENT

This part is about the Man Management I observed and experienced within the IT department of TotalFinaElf Gas&Power London.

2.1. Working conditions

In every department of TFE Gas&Power London, the office is organised as an open space. We also find this disposal in the IT department. There is one main desk for six people and two smaller desks for two-three people each. I think the open space office enables to make easier the communication between the people and therefore to improve the work atmosphere and the team work. However, the environment is sometimes noisy (photocopier, laughing…) which can disturb the concentration.

Concerning the work hours, it can be sum-up by the word ‘flexibility’. Due to the IT business, we must be ready to complete tasks during the out-of-work hours. Besides some of us must be reachable all the time. Every week, two members of the staff are “on call”, that is to say they are the people to contact (in case of problems) during nights and weekends. On the other hand, there is no problem during the day to go out the office for a short time. For example, you can take a break for buying some food or going to the bank. Personally, my work hours were generally 08:30am until 06:00pm. We had about a one-hour break for lunch.

With these observations, I felt one trait of the Anglo-Saxon mentality, which is ‘flexibility and results’.

2.2. Employee’s Contracts

There are five contracts for the people of the IT Staff. We find temporary, consultant, VIE, local and expatriate contracts. I would like to stress that only four people out of ten are really employed by TotalFinaElf. One of the reason of the externalisation of IT services is flexibility. Before the merger of TotalFina with Elf, there were two IT services in London Cavendish: one for the development and one for the infrastructure. After the merger, the two services have been gathered and the IT team was completely renewed.

I noticed that the turnover is relatively low at TFE London. Some people come and go but it is often to go in another TFE site. As a matter of fact, there is few ‘Escape of competencies’.

I think we can find more employment with fixed-term contract in the UK because it is easier in the UK to renew the contracts when hired through an Agency. Moreover the ‘flexibility’ is part of the Anglo-Saxon culture.

Concerning the ‘Expatriate’ contract it is for TFE employees of France who work abroad. They are paid in France and are lodged by the company in the foreign country. This contract is very advantageous for motivated people who are looking for an international experience. As a French trainee, I had a status similar to ‘Expatriate’ because my contract was in France and because the company gave extra money for the accommodation. There are several trainees at TFE London and especially in the GRC (Geoscience Research Centre) department.

2.3. Courses and Bonuses

Philippe Guelminger, the IT manager, thinks it is a good thing for the employees to attend at least one technical course per year. It depends on wishes of the staff: some of them prefer to get more knowledge by attending courses others by reading books. The courses are proposed by companies, which are specialised in the education.

I had the opportunity to attend several seminars or conferences about network security. These seminars were not real courses but it was a good approach to get knowledge on technologies.

TFE also offers internal training in their headquarters in Paris. They propose both technical and managerial courses. The managerial courses are reserved for the people who have managerial abilities.

The employees are awarded for their work by bonus systems. The Human Resources defines the rules to calculate these bonuses. The parameters to calculate the bonuses are the company results, the individual results and the manager assessments.
TotalFinaElf is a world-wide company with various activities. If an employee wishes to go on another site, he/she is encouraged asking to his/her manager. The "Career mobility" department in Paris can examine his/her request. They examine and decide what are the strategic choices to move someone on another site.

2.4. Career evolution and relationship with the hierarchy

- Hierarchy

The Hierarchy is quite structured in the IT staff as well as in the other services. I was a little astonished of that because I heard the hierarchy is generally on one level in Anglo-Saxon countries. I think the reason is that it depends on each company and that TotalFinaElf has kept its French culture of hierarchy. Philippe is the IT manager, he is responsible of all the service. Cedric is the Project manager, that is to say he supervises every operations for TFE G&P London. Chris is the IT support manager, he manages the two people support staff.

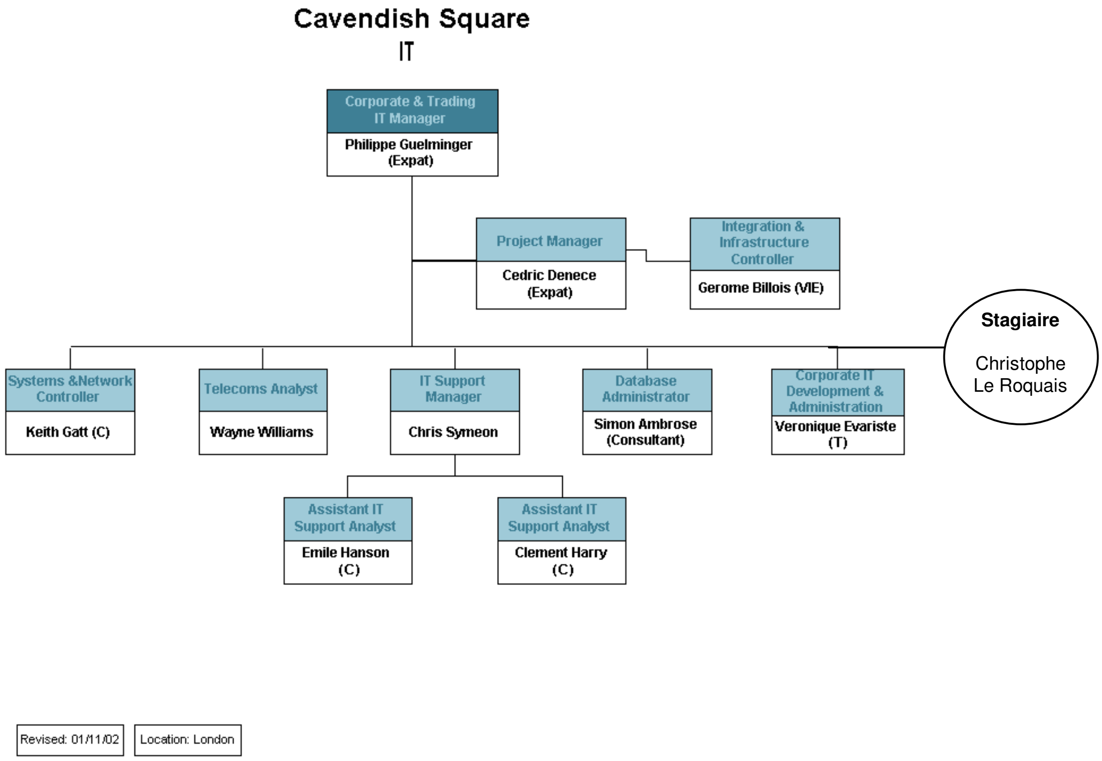


Fig. 2: IT Organisation Chart

- Competencies assessment and career evolution

Philippe organises an annual personal assessment every September. This is the opportunity to talk about the projects in the past and in the future. Philippe checks if the objectives have been reached and he defines the objectives for the following year. After this meeting, Philippe gives his assessment to the London head manager.

2.5. Communication within the staff

I think the communication is one of the main points in Man management. The manager is the gateway between his team and the hierarchy. He must have the abilities to give the good information to the good person at the good time.
When arriving in a new company, I find it is good to receive a 'Welcome Booklet' which presents the company. It is also nice to attend a presentation meeting with the other new employee. When I arrived in September, I was a little astonished not having received a 'Welcome Booklet'. However, I got managed to have more information about the company's activities by questioning people in the trading room. It enabled me to get in touch quickly with the employees of the other departments.
The Intranet of the company is a real work tool. It has information for the business like Market Indexes. It is also a communication tool because it has a phone book and a web mail access.
With the staff, I communicated mainly by talking since we all were in the same room. In addition to speaking, I also sometimes used the email. It is sometimes easier to communicate technical details by e-mail.
For important things like project designing, I organised small appointments with Philippe or Cedric.

2.6. The meeting leading

Philippe generally organised a meeting with all the IT staff once every three weeks. Before the meeting, he prepared an agenda. I think it is necessary to prepare an agenda because it enables to lead a direct and efficient meeting.
For the IT staff meetings, Philippe asked to each of us the one after the other if the tasks were completed and what was the advancement of the projects. Every meeting lasted about forty five minutes and I can say it was useful because it enabled us to get informed about the other's projects. Moreover, this is a good way for the manager to evaluate the costs of the projects and to organise the future ones.
For keeping tracks of the meetings, each of us noted information on his book. There were no minutes for these meetings.
During my training period, I was the client for a project to integrate a new network in our site. I wrote a tender and sent it to several consulting companies. I was responsible for managing the meetings with these consulting companies. I got managed to arrange an appointment with them and prepared an agenda. During the meetings, I answered to their questions and I insisted on the important points of our tender. For example, I stressed the point concerning the support we expected. Our meetings lasted about half an hour and sometimes it was a phone conference.

2.7. The role of the managers

I worked in an efficient team where the atmosphere was very good. I think Philippe played an important part in this. He always was ready to hear each of us, and to talk to us with a pleasant way. He was very closed to us, ready to joke. I think the role of the manager is to be able to take decisions, to well-manage a budget, to motivate the team, to delegate intelligently tasks, to cope with the conflicts. In addition to that, he must have the human qualities of socialising and charisma. I can honestly say that I found all these qualities by Philippe and Cedric.

3. TECHNICAL PART

3.1. Projects Management

3.1.1. Training Subject

When I met Michel Guillé and Philippe Guelminger in May 2002, we talked about headlines of my mission. I knew I would be mainly involved in a VPN project but no further details were given during the initial discussions..
At the beginning of July 2002, I asked Philippe Guelminger to send me the detailed training subject by e-mail. I received the following on July, 12th:

> The scope of this training is particularly wide and requires a full commitment of the trainee, as due to the business, some jobs could occur during weekends.
>
> 1- To implement and test a VPN and strong authentication connection between clients and main network through Internet and RAS. You will have to use the technologies as below:
> - RSA SecureID
> - VPN Checkpoint1
>
> To provide with the appropriate procedures
>
> 2- To develop and design templates and groupware applications based on Lotus Notes 5. To provide with the appropriate procedures.
>
> 3- To participate to the day to day IT support of an energy-trading floor.
>
> This training is located as below:
> TotalFinaElf Gas and Power Ltd
> 33 Cavendish Square
> London W1G0PW UK

TotalFinaElf Gas&Power had little knowledge of the new VPN technology. They wanted to get acquainted with the technology in order to provide home-employees with a future secured remote VPN access over the Internet. This is the reason why the goal of my main responsibility was to focus on VPN technologies especially with RSA SecureID and VPN Checkpoint.
Thanks to the Public Offer Project in 4TC, I already had knowledge on VPNs. However, I knew I had to get more documentation particularly on the manufacturer's solutions to enhance my knowledge.
The second point of the training subject was to design Lotus Notes templates. Philippe noticed on my CV that I had already hands-on-experience on Lotus Notes (I was the Lotus Notes administrator during my third-year training-period). Lotus Notes is relatively recent at TFE Gas&Power and they may needed assistance in the design of templates.
On top of these projects, I was to help with the IT support, that is to say, set-up computers, answer the helpdesk phone, fix hardware and software problems…

3.1.2. Planning details

In the few days following my arrival at TotalFinaElf, I met Philippe in order to clarify my job description and to establish a work plan. I think this is very useful because it fixes deadlines and therefore it enables me to know what is expected.
Philippe wrote the details down on the following memo:

VPN:
mid - october : market study about VPN solution (including Cisco and Nokia checkpoint), including strong authentication (RSA)
- for client and site to site connection
mid - november : price comparaison, proposal
by the end of november : presentation to IT department

IDS:
mid november : market study, comparaison of the different equipment . Targeting a low cost and easy administration solution . Intrusion detection should cover internet hacking.
by the end of november : presentation to IT department

end november, december : Test some products (trial period)

+ taking part of the trading support.

Philippe GUELMINGER
TOTALFINAELF GAS & POWER Ltd
Corporate and Trading IT Manager
+44 (020) 7318 6838 (W)
+44 (0)7909997262 (M)
+44 (0)8705275212 (fax)
philippe.guelminger@totalfinaelf.com

For the VPN project, at first I had to carry out a market survey on VPN solutions for both client-to-site and site-to-site connections. It had to be a global survey both technically and economically as well as a comparison with existing remote accesses.
Having talked about Lotus Notes templates with Philippe, it turned out that they no longer required my help as a colleague was already working on it. However, Philippe told me that the group wanted to set-up an IDS-like solution (Intrusion Detection System) for security purposes. Their main preoccupation was to find a solution to analyse automatically the firewall logs and to alert the network administrators when detecting an intrusion attack.
I knew nearly nothing about IDS before but I took part in this project because I felt it would be very interesting.

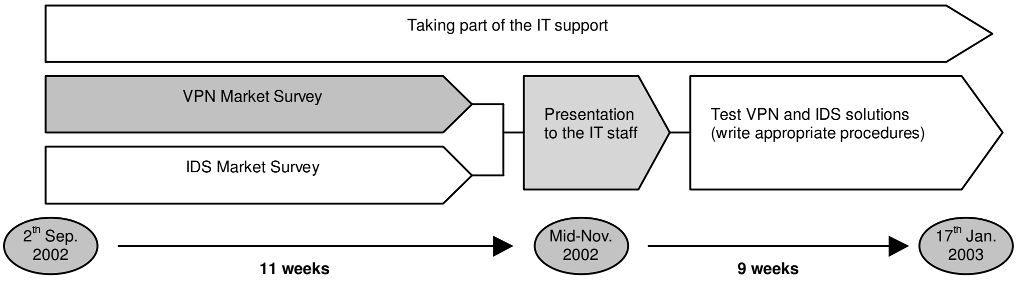

Taking part of the IT support
VPN Market Survey
IDS Market Survey
Presentation to the IT staff
Test VPN and IDS solutions (write appropriate procedures)
2th Sep. 2002
11 weeks
Mid-Nov. 2002
9 weeks
17th Jan. 2003

Fig. 3: basic work plan

3.1.3. Additional Projects

Obviously, the training topic was not necessarily restricted to the above mentioned projects; other tasks could be done when demanded. In addition to the VPN project, the IDS project and the IT support, Philippe wanted to give me another wide project: the '**Nomade Project**'.
We met together in early November to discuss this project. The situation was that Paris wanted to setup a new dedicated network for securing the remote access of the Gas&Power

marketers. A large study was carried out by Paris and all the elements to build the network were given. My task would be to write a tender from the Paris documents and to be in touch with the local suppliers.
In this project, which was not very technical, I would play the role of the client for a public offer.

At the end of November, Philippe received a '**Trading Assessment**' file from Paris. Paris asked us to fill in the Excel File concerning our IT devices. The file contained very accurate questions with details like "Are your external WEB systems connected to internal databases?"
To answer all the questions, I asked every member of staff to help me to answer the questions that related to their field of competence. Some questions were related to the Houston (USA) site. I contacted the IT manager in Houston these questions to answer.
Please refer to *Appendix A* to see the model of the Trading Assessment sheet.

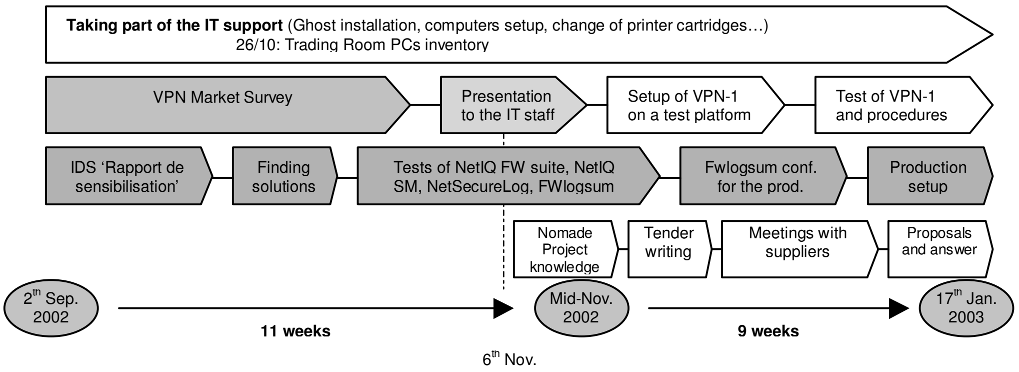

Taking part of the IT support (Ghost installation, computers setup, change of printer cartridges…)
26/10: Trading Room PCs inventory
VPN Market Survey
Presentation to the IT staff
Setup of VPN-1 on a test platform
Test of VPN-1 and procedures
IDS 'Rapport de sensibilisation'
Finding solutions
Tests of NetIQ FW suite, NetIQ SM, NetSecureLog, FWlogsum
Fwlogsum conf. for the prod.
Production setup
Nomade Project knowledge
Tender writing
Meetings with suppliers
Proposals and answer
2th Sep. 2002
11 weeks
Mid-Nov. 2002
9 weeks
17th Jan. 2003
6th Nov.

Fig. 4: Final planning

3.2. VPN Project

3.2.1. VPN Market Survey

- Gathering Information

The first step of my training was concentrated on the VPN Market Survey. The main goal was to study the advantages of the VPN technology for providing remote users with a secured connection and that from anywhere.
First, I had to get more information on VPN technologies. I obtained theoretical knowledge from the Internet and the Checkpoint VPN manual. With Cedric, we also had an appointment with Netconnect (TFE G&P IT consultant company) on October, 22th. They gave us interesting facts on VPNs.To carry out my survey, I had to know what the existing remote connections were at TFE G&P. For that, I questioned Philippe Guelminger and Cedric Denece. Then, I had to compare the current remote access technologies with the VPN one, especially in terms of throughput, security, QoS and costs.
To get information about the manufacturer's solution, I found all the necessary specifications on the manufacturer's websites.

- Contents

The "Market Survey for implementing a Virtual Private Network" is put in *Appendix B*. I spent about four weeks working on the market survey and I learned a lot on TFE G&P remote accesses, on the VPN technologies and on the VPN leader's solutions.
The Market survey deals with the VPNs over the Internet with the price-estimates. One part is about 'Clientless VPN' which enables the remote users to connect to the LAN without installing a client application. Philippe wanted to get more information on these possibilities because they can be useful when connecting from an Internet Café for example.
I would like to stress that the Citrix NFUSE solution is very interesting because it allows access to remote applications with only the Web browser. Thus it is not necessary to setup a client application on the client computer.

- Presentation to the IT staff

Having prepared the VPN market survey report, I organised an appointment with the staff to present my work. This type of presentation happens regularly at TotalFinaElf. It enables all the staff to get informed about colleagues' projects.
I presented my work on the 6th November 2002. My presentation was comprised of 24 slides and lasted about 45 minutes. I did it in English, which was not an easy task. I think all the staff was interested. They asked me several technical details at the end of the presentation.

3.2.2. VPN Tests with Checkpoint FW-1/VPN-1 NG FP3

After my presentation, we decided with Philippe to test Remote VPN accesses with Checkpoint FW-1/VPN-1.
As we did not have the latest version of Checkpoint, I contacted the Netconnect company in order to receive an evaluation of Checkpoint FW-1/VPN-1 NG FP3.

- Test Environment

To test the Checkpoint VPN features, I designed a network architecture test. The external VPN server network card was connected to the Trading LAN and I created my own network on the Internal VPN server side. The architecture test platform was as follows:

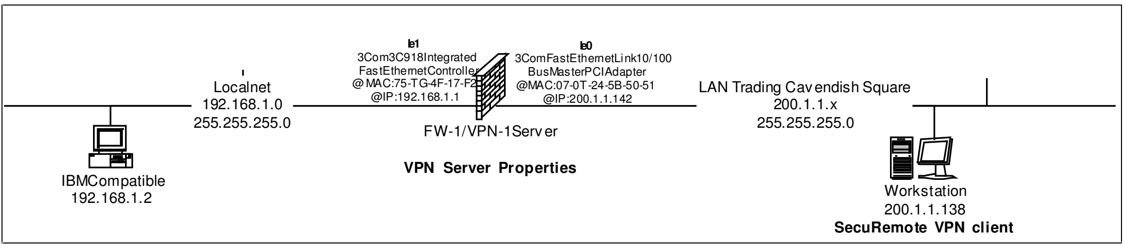


Fig. 5: VPN test architecture

VPN features I chose to implement were:
- Encryption scheme: 3DES
- Authentication: Shared Secret
- Integrity: SHA-1

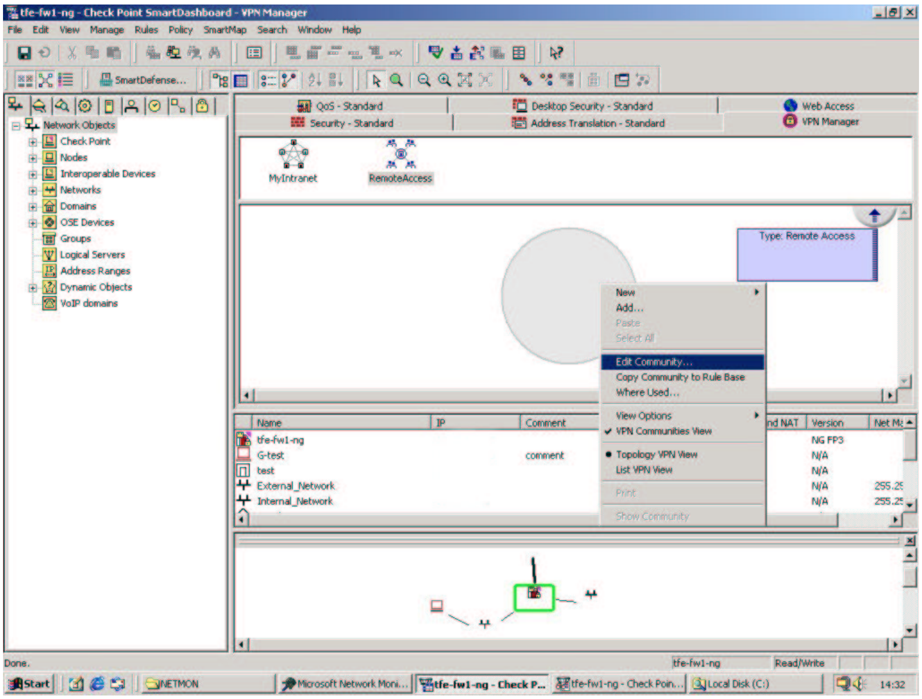
- Setting-up the Checkpoint FW-1/VPN-1 Server

To set-up Checkpoint FW-1/VPN-1, I first took a PC and I installed Windows 2000 Server on it. Then I carefully configured network cards and other network parameters. It is very important to configure them properly since Checkpoint automatically gets these pieces of information to pre-configure its properties.
The installation program guides you step by step. It is quite easy to install the checkpoint software.

- Configure the VPN Server

To configure the VPN Server, we must:
- Create a user group and configure the authentication method for each user of the group
- Create a VPN gateway
- Configure the encryption, integrity and authentication properties on the VPN server

Please refer to *Appendix C* to see the VPN server installation procedure.



Name	IP	Comment	nd NAT	Version	Net M
tfe-fw1-ng				NG FP3	
G-test		comment		N/A	
test				N/A	
External_Network				N/A	255.2
Internal_Network				N/A	255.2

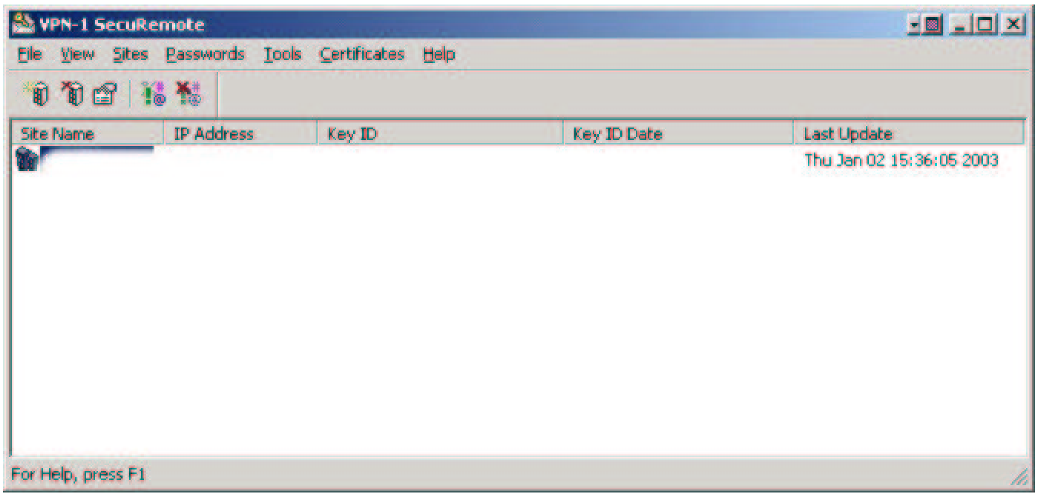
Fig. 6: the window to configure the VPN Server

- Configure the Client

The Checkpoint VPN client for Remote users is SecuRemote/SecureClient. SecuRemote is a simple VPN client whilst SecureClient has additional personal firewall features. These properties are called 'DesktopSecurity'. These rules can be configured from the VPN server and they are able to minimise threats through the VPN tunnel.

I set-up a SecuRemote client on a test machine. The installation software package is freely downloadable at http://www.checkpoint.com/techsupport/downloads_sr

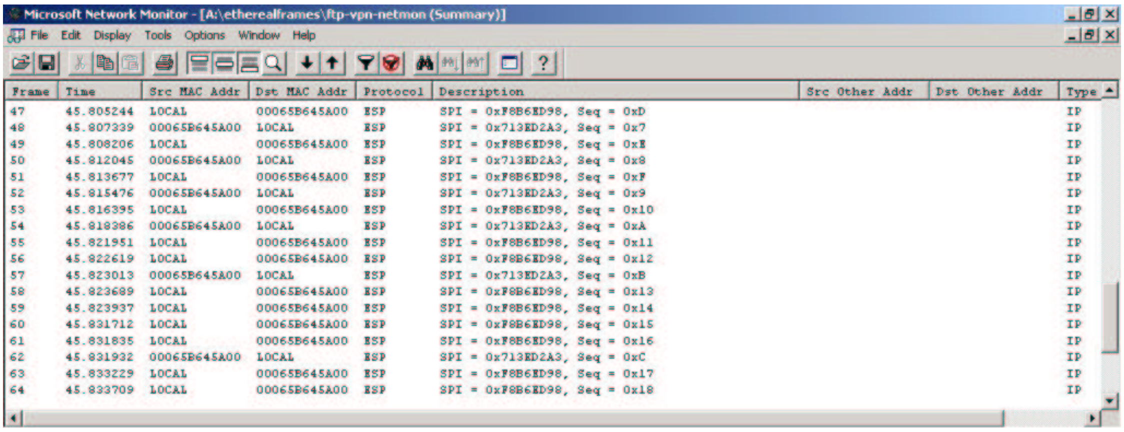
The main action to configure SecuRemote is to enter the IP address or the name of the VPN Server. The VPN Server sends back to SecuRemote the VPN parameters and especially the VPN network topology. Please refer to *Appendix D* to see the VPN client installation procedure.



Site Name	IP Address	Key ID	Key ID Date	Last Update
				Thu Jan 02 15:36:05 2003

Fig. 7: the SecuRemote Window

To check that the encryption was enabled, I captured frames from the Firewall external Ethernet Card. As we can see on Figure 8, Data are encapsulated in ESP tunnel Mode.


Microsoft Network Monitor - [A:\etherealframes\ftp-vpn-netmon (Summary)]
File
Edit
Display
Tools
Options
Window
Help
?

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Other Addr	Dst Other Addr	Type
47	45.805244	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0xD			IP
48	45.807339	00065B645A00	LOCAL	ESP	SPI = 0x713ED2A3, Seq = 0x7			IP
49	45.808206	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0xE			IP
50	45.812045	00065B645A00	LOCAL	ESP	SPI = 0x713ED2A3, Seq = 0x8			IP
51	45.813677	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0xF			IP
52	45.815476	00065B645A00	LOCAL	ESP	SPI = 0x713ED2A3, Seq = 0x9			IP
53	45.816395	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0x10			IP
54	45.818386	00065B645A00	LOCAL	ESP	SPI = 0x713ED2A3, Seq = 0xA			IP
55	45.821951	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0x11			IP
56	45.822619	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0x12			IP
57	45.823013	00065B645A00	LOCAL	ESP	SPI = 0x713ED2A3, Seq = 0xB			IP
58	45.823689	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0x13			IP
59	45.823937	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0x14			IP
60	45.831712	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0x15			IP
61	45.831835	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0x16			IP
62	45.831932	00065B645A00	LOCAL	ESP	SPI = 0x713ED2A3, Seq = 0xC			IP
63	45.833229	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0x17			IP
64	45.833709	LOCAL	00065B645A00	ESP	SPI = 0xF8B6ED98, Seq = 0x18			IP

Fig. 8: the encryption flow

3.3. FW logs analysis

3.3.1. Gathering information

While writing the VPN market survey, I had to get information about IDS products and which ones could fit our needs. Our ideal requirements were to set-up an application to centralise and analyse automatically logs and alerts from the various network devices (firewalls, switches, routers, and servers). The highest priority was to summarise and to analyse the Firewall logs since it generates tens of thousands entries per day.
At the beginning of my training, we met the ISS company (www.iss.net) who are the leaders on the IDS market. They presented us with their products. It was very interesting because I knew nothing about IDS products before. However, it turned out that their solution was too huge for our needs and that it required too much maintenance.
I wrote a document named "Intrusion Detection Systems: Rapport de Sensibilisation" to clarify the state of the art. Please Refer to *Appendix E* to see it.
I carried out a search on the Internet to find solutions corresponding to our needs. I decided to test NetSecureSoftware NetSecureLog, NETIQ Reporting Center, NETIQ Security Manager and Fwlogsum.

3.3.2. Tests of the possible solutions

- NetSecureSoftware NetSecureLog

NetSecureLog is a piece of software to centralise logs from firewalls, IDS, routers and proxies in an Oracle database. The administration console is a web interface. The administrator can find critical events by processing requests.
We must install an agent on each device we wanted to take the logs. A management service stores data in the database.
I tested this solution for about two weeks and I thought it did not completely answer our needs. The use of an Oracle basis requires a powerful PC and the system of requests is not user-friendly.

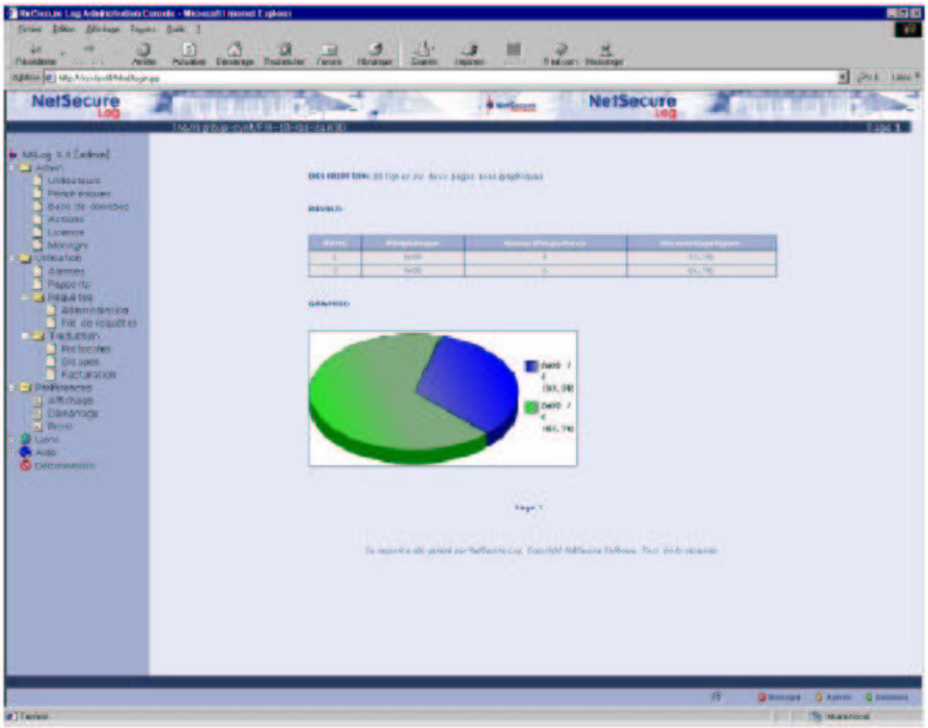
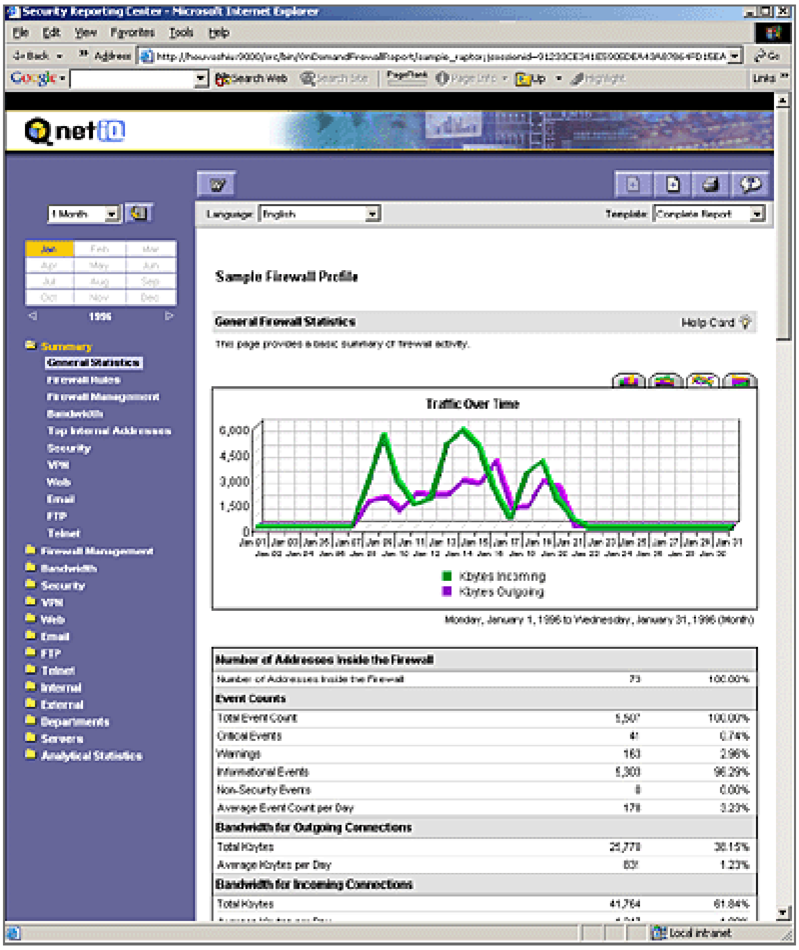


Fig. 9: NetSecureLog Administrator Window

- NetIQ Reporting Center

NetIQ Reporting Center is the equivalent of WebTrends for Firewalls and Proxies. It processes log summarisation from the firewall and proxies logs. It is compatible with most of the firewalls and proxies available on the market.
In addition to classify logs according to their Source IP addresses, their Destination addresses, their services,… It delivers data on the bandwidth and makes 3D graphs.
I think this product is very good because it is user-friendly for the end user. However, it delivers maybe too much data (sometimes redundant) and it is very expensive (£6,000).



Sample Firewall Profile

General Firewall Statistics

This page provides a basic summary of firewall activity.

Monday, January 1, 1996 to Wednesday, January 31, 1996 (Month)

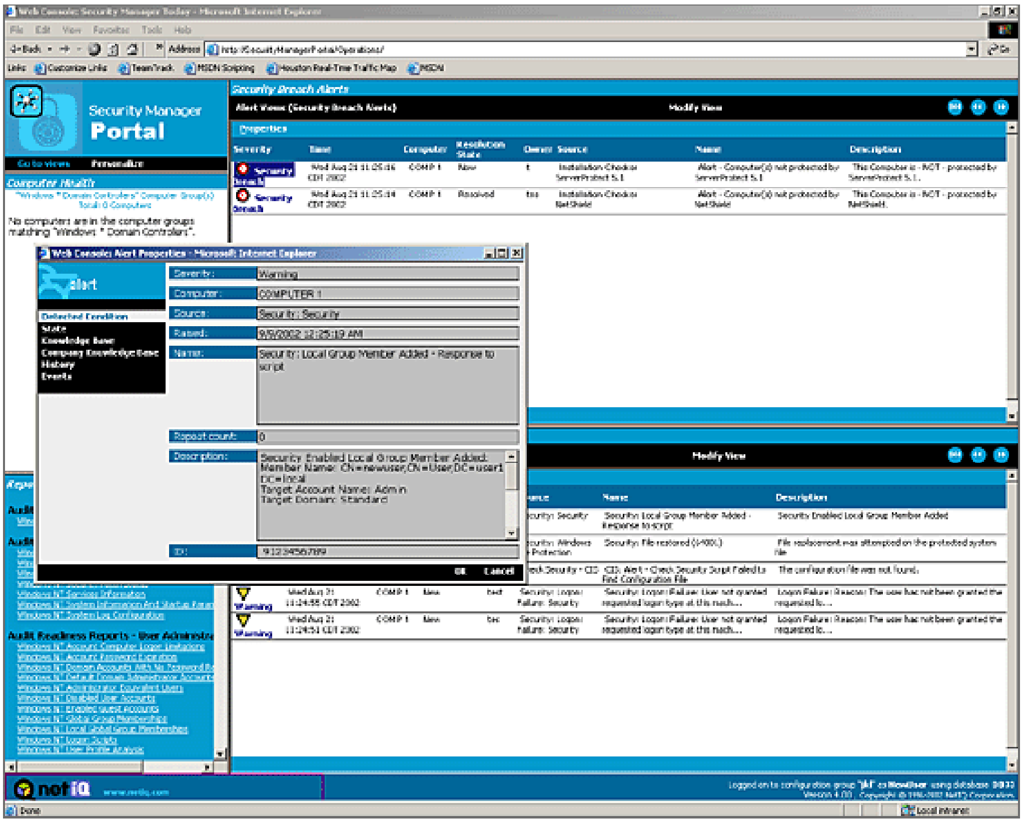
Number of Addresses Inside the Firewall		
Number of Addresses Inside the Firewall	73	100.00%
Event Counts		
Total Event Count	5,507	100.00%
Critical Events	41	0.74%
Warnings	163	2.96%
Informational Events	5,303	96.29%
Non-Security Events	0	0.00%
Average Event Count per Day	178	3.23%
Bandwidth for Outgoing Connections		
Total Kbytes	25,779	38.15%
Average Kbytes per Day	831	1.23%
Bandwidth for Incoming Connections		
Total Kbytes	41,764	61.84%

Fig. 10: NetIQ Security Reporting Center

- NetIQ Security Manager

NetIQ Security Manager is a complete solution to administrate Network devices such as servers, firewalls, IDS or proxies. We must set-up an agent on the device we look after and Security stores the logs in a central database (MS SQL Server). Security Manager has a lot of pre-activate alerts. For example it warns the network administrator when a well-known security flaw is detected on a device. We can also create the alerts we want to generate and the way in which they happen (Mail, SNMP trap, sound).
The supervisors can access the central management either by the application on the manager host or by the web interface. The interfaces are user friendly and we have the possibility to generate Excel or Word reports.

Security Manager is really a command center to centralise all the network security problems. Its functionality is huge. On the other hand, it is heavy, requires lots of time to maintain and to administrate and it is very expensive (£1,000 per device to look after).



Security: Warning
Computer: COMPUTER 1
Source: Security: Security
Raised: 9/9/2002 12:25:19 AM
Name: Security: Local Group Member Added - Response to script
Repeat count: 0
Description: Security Enabled Local Group Member Added: Member Name: CN=newuser,CN=User,DC=user1 DC=local
Target Account Name: Admin
Target Domain: Standard
ID: 9123456789

Fig. 11:NETIQ Security Manager Web Interface

3.3.3. Best solution: FW Logsum

Fwlogsum is a Perl script to summarise FW logs making it easier to see what services are being blocked or allowed through the firewall. It provides many sorting and filtering options and also handles address/port translation. In addition, it can also handle logs from other firewalls and many others by using a converter.
It can be freely downloaded at http://www.ginini.com

Fwlogsum can process text or html reports. It requires a FW log in ASCII format as an input file. This FW log file can be obtained by processing the '`logexport`' command on the FW Management server. Reports show logs and statistics. The script requires perl5.0 or higher.

In addition to the firewall log summarisation, we wanted to save our firewall logs.
We had the choice either to backup the binary logs or to backup the ASCII logs. We have decided to backup the ASCII logs because they are easier to exploit.
Considering the big size of the ASCII log files (about 30 Mbytes each) they will be compressed before the backup (compression rate: 95%).

3.3.4. Architecture and implementation

The architecture we have setup is as follows:

- Installation of a dedicated machine (named 'CTRSERVER') in the Management DMZ (the DMZ where the FW Management Server is).
- The conversion of FW binary logs into ASCII happens on the FW Management Server.
- On the CTRSERVER, we store the FW ASCII logs, we run the `'Fwlogsum'` script to process HTML reports. HTML reports are stored in a directory, which is the root directory for the IIS server.
- An agent installed on the Domino Sever sends the http link to the new html reports to the controller's mailbox daily. This makes easier it to access the new html reports.
- A robocopy job copies the FW ASCII logs from 'CTRSERVER' to 'APPS'. Since 'APPS' is backed-up on tapes, FW ASCII logs are consequently saved on tapes.
- We have installed a new rule on the Firewalls to allow the controllers to access 'CTRSERVER' and especially the HTML reports.

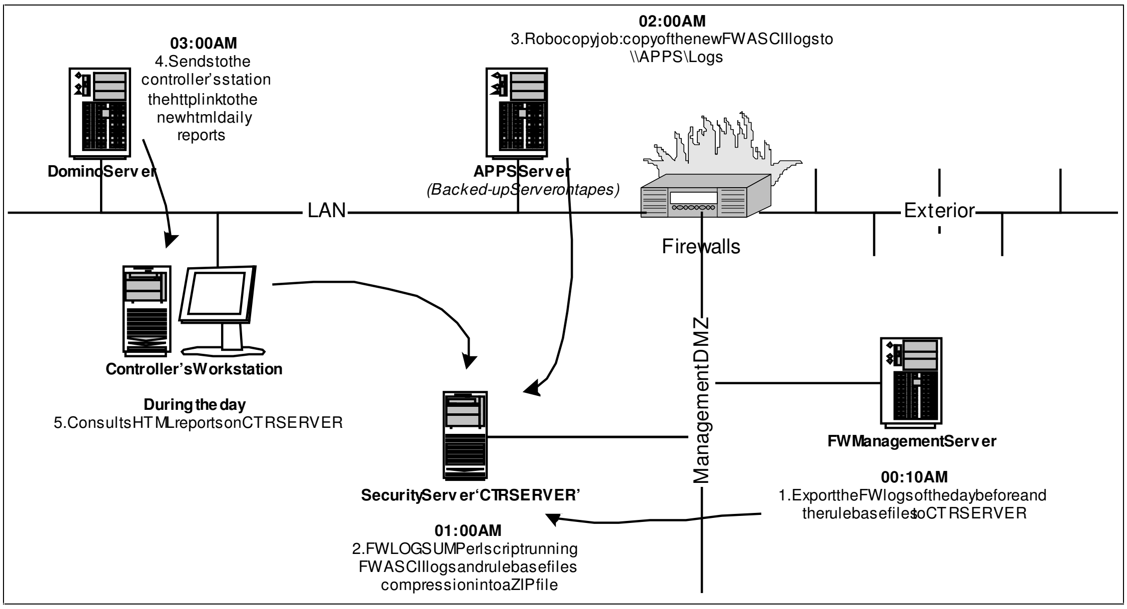

03:00AM
4. Sends to the controller's station the http link to the new html daily reports
Domino Server
02:00AM
3. Robocopy job: copy of the new FW ASCII logs to \\APPS\Logs
APPS Server
(Backed-up Server on tapes)
LAN
Firewalls
Exterior
Controller's Workstation
During the day
5. Consults HTML reports on CTRSERVER
Management DMZ
FW Management Server
Security Server 'CTRSERVER'
00:10AM
1. Export the FW logs of the day before and the rulebase files to CTRSERVER
01:00AM
2. FWLOGSUM Perl script running FW ASCII logs and rulebase files compression into a ZIP file

Fig 12: Architecture set-up for FW logs analysis and backup

00:10 AM	01:00 AM	02:00 AM	03:00 AM
FW Mangt Server	**CTRSERVER**	**Domino Server**	**Robocopy**
fwlogexport script running .	fwlogsum script execution ASCII logs compression	Send the Controllers mailbox the link to the new HTML reports	copy ASCII logs on APPS

To process automatically and dynamically the above tasks on the 'FW Management Server' and on 'CTRSERVER', we have written two VB scripts: `'Fwlogexport.vbs'` on the Management Server and `'Fwlogsum.vbs'` on 'CTRSERVER'.
The installation procedure with the VB scripts are put in *Appendix F*.

3.4. 'Nomade' Project

3.4.1. Get the pre-existing study and writing of the tender

Paris HQ requested a study from a consultant company to provide them with recommendations for making secured the remote users' laptops.
I referred to the document called "Referentiel de securisation du poste de travail Nomade" at the beginning of November. The 124 page document analyses the different existing solutions at the different levels of security and concludes by recommending some products.
I used this document to write the tender destined for the potential local integration companies.
The security of remote laptops must be manageable from a central network, which is being set-up in the Cavendish Square site. The various solutions we have adopted are:

- Zonelabs Integrity Server for updating the personal firewalls and Antivirus
- Cisco VPN Server to establish the VPN connection between the laptop and the corporate network.
- ActivCard for storing passwords and authenticates
- Checkpoint/NOKIA firewall for securing the network
- Cisco Pix firewall for doubling the security

Through the writing of the tender (The tender is in *Appendix G*), I learned what the possible solutions for securing remote hosts are and how to consider financial/organisational points. For example, Philippe stressed the fact that Support questions must be clearly exposed in the tender.

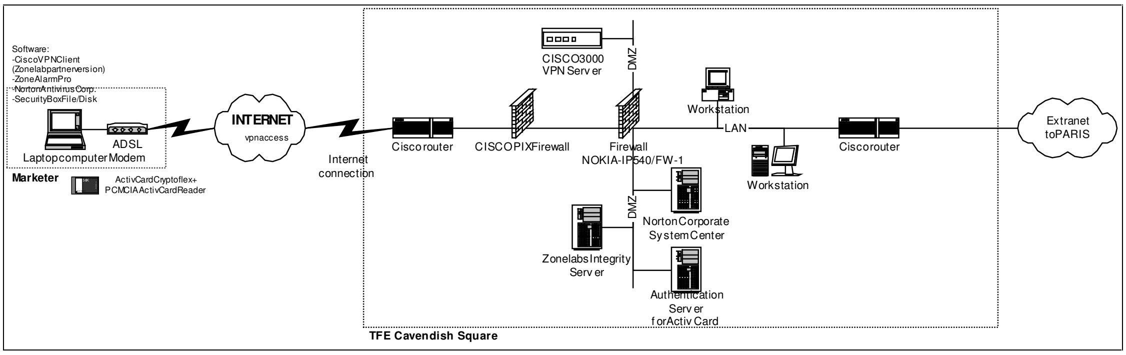


Fig. 13: Nomade Prospective Network

3.4.2. Meetings with the Integration companies.

Mid November, I sent the tender to eight integration companies asking them to answer before Christmas.
Having received the tender, many of the integration companies wanted to meet us in order to get more information.
From the end of November until mid December, I received representatives from seven integration companies at our office. I was sometimes with Philippe, Cedric or Gérôme and sometimes alone. I was in charge of organising these meetings and managing them. Most of the questions were technical and sometimes asked by phone by one of their colleagues. Other questions were organisational for example: "Do you want us to we pre-configure the network devices in our labs or directly on your site?"

3.4.3. Integration companies' proposals and our decision

The week before Christmas, we received four proposals for our tender. Their proposals were quite similar but I noticed differences especially concerning the cost. The cost for the consulting could reach differences of 20,000 €uros.

Paris was the real client for this project since it was a project for the Corporate. Having received the proposal from the integration firms, I sent them to Michel Guillé, IT Director in Paris.
The decision to choose the supplier company is taken at the end of January therefore I had not the opportunity to assist at the beginning of the network integration in our site.

3.5. IT Support

3.5.1. Day to Day basis tasks

- Ghost image installation

When setting-up a new computer, we use ghost images. A ghost image is a pre-configured file, which is specially designed for a service and quick to install. It specifically contains the Operating System.
Clement showed me how to use Norton Ghost to get the adequate image from the network. During my training, I set-up a ghost image on three separate occasions.

- To connect a PC to the LAN

There are network plugs in the ground. To connect a computer to the LAN, we must connect the cable from the computer to plug in the ground. Then, the connection must be done in the common rooms between the storey hub and the LAN switch.

- Other tasks

Change a cartridge in a printer, setting-up of a trading software, unblock a paper-jam in a printer...

3.5.2. Trading Computers Inventory

As mentioned in my training specification, it was possible that sometimes I had to work during weekends. IT requires flexibility because some tasks must be done out of the working hours. For example, I went to work on Saturday 26th October because we had to do the inventory of the computers in the trading room. I wrote references of every screen and central units and saved this data in an excel file. It was a long process (60 computers with about 4 screens for each of them).

Conclusion

This training-period was a great opportunity for me. It has enabled me to get hands-on experience in a multinational firm. Once again, I am grateful to Michel Guillé and Philippe who gave me the chance to work at TFE London. Life and work conditions were perfect. I had no problems with the accommodation or with the opening of a bank account thanks to the help of Charlotte Nosworthy (Human Resources Advisor). At the office, I worked with a very pleasant team from whom I learned a lot. We had great moments together at work and outside. I think the social life with colleagues is more developed in the U.K. To go to the pub after work or having a Christmas Party with colleagues are part of the British traditions.

Technically, it was really worthwhile. I improved my knowledge in networking and computing. I am convinced that the projects I led have been useful for the company.

This training-period was really great and I hope that another TC student will have the opportunity to get such a training period in the coming year.