

Design Case - Fake Consulting

Stian Jahr

September 2005

1 Abstract

This paper will make a design for Fake Consulting Inc(from now: FC). The goal is to go through the design process and produce an usable design based on the case given in [Tor04a].

2 Introduction

FC already got some perimeter security. They got a statefull firewall with four interfaces connected as in figure 1. To help me with designing the perimeter security I've chosen some of the design principals from Saltzer and Schroeder[Bis03]. Saltzer and Schroeder's principals are the most fitted principals for perimeter security. [Gol99]'s design principals is more holistic principals and focus on complete systems and does not fit well into perimeter security. [VM02]'s design principals are quite similar to Saltzer and Schroeder's principals, so I will only pick design principals from Saltzer and Schroeder. The three principals I found most relevant are these:

- *2 - The principle of fail-safe defaults.* This means that unless a subject is given explicit access to an object it should be denied.
- *3 - The principle of economy of mechanism.* The security mechanism should be as simple as possible. This harmonize with FC's CFO¹ focus on cost efficiency.
- *8 - The principle of psychological acceptability.* The users of the system are fraud management consultants, and not IT experts. The solution should require low IT knowledge threshold. In best case, the user just push the "secure me" button, or don't do anything at all.

The other design principals are also relevant as well, but these are in my focus of the design.

¹Chief Financial Officer

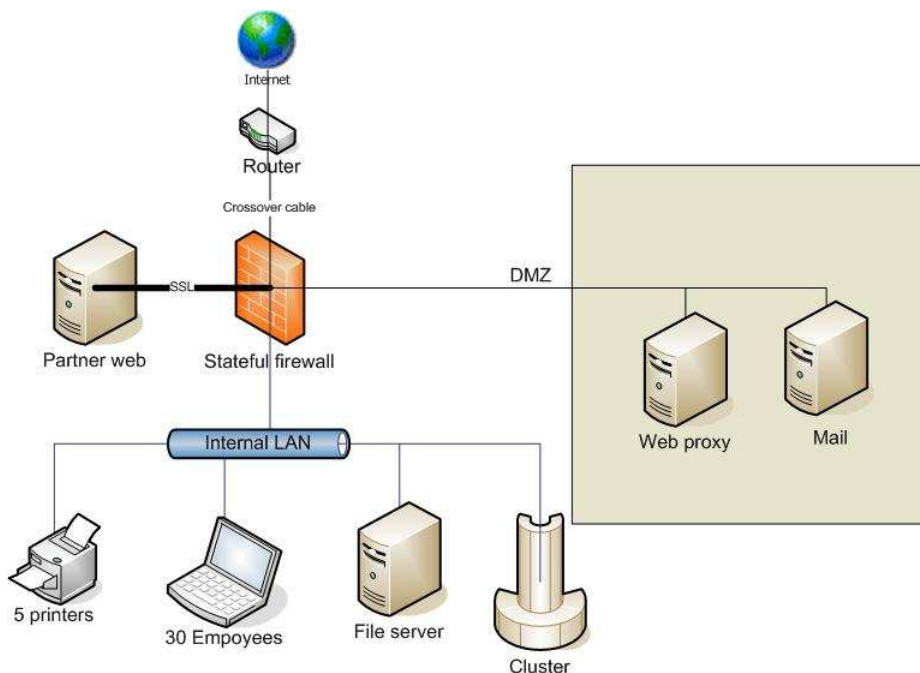


Figure 1: Current perimeter security of FC

3 Intrusion Detection System

3.1 What is IDS?

The current solution of FC doesn't include IDS. They want to know if and how IDS can be used to strengthen their over all security.

An IDS scans the network traffic for suspicious activity. There are two ways of detecting these activities: signature based and abnormal based. The signature based IDS looks for known malicious network traffic, for instance:

```
GET /scripts/../../../../winnt/system32/cmd.exe?/c+dir
```

This is the signature of the Nimda worm [NWF⁺03]. When this HTTP request occur on the network traffic the IDS should stop the request. This will help you stop the traffic known bad, but it can't stop new worms or hackers. However some script kiddies will be stopped, because they use known hacker tools with known signature. To stop new worms and hackers the IDS can determine if the network traffic is normal. Than you get the problem: what is normal? This require training of the system to fit in your environment.

When the IDS detects suspicious activity it somehow react. Either passive or active. Passive response means just create a log of the IDS alarm. Then a

system administrator must go through the log and take action based on what the log tells him. This does not increase the security of the system directly, but it can come in handy when you set the rules of the firewall, investigating after an attack and last but not least detect a planned attack in an early phase. If an attack is detected in the recognition phase, the system administrator can take action to prevent the attack. This can also be done automatically. If the IDS for instance changes the rules of the firewall temporary or permanently it contributes to increase the security. However this is not an IDS anymore, the name has changed to Intrusion Prevention System.

3.2 Does an IDS increase FC's perimeter security?

An IDS indirectly increase the security, but it needs to be watched by a system administrator. Dependent on the strict the IDS is there will be false positives and false negatives. Be ware of these. Don't react on each alarm and don't feel secure because the IDS hasn't alarmed you.

There are two different locations to place the IDS. Either on the host or in the network. In this case I find it appropriate to place the IDS in the network. The laptops the fraud managers uses in the customers premises will be secured with a personal firewall with high restrictions (see section 5).

The traffic before the firewall is often not interesting. The interesting traffic is what comes through the firewall. I would recommend the solution on figure 2. As you see I've placed an IDS with three sensors and an IDS console in the network. These sensors are placed at the firewall interfaces without the one connected to the Internet, and looking for suspicious network activity which has passed the firewall.

4 Virtual Private Network

FC's solution today is based on VPN in OSI layer 7 (SSH). They need to use SSH to reach the web-proxy in the proxy-network and telnet from the web-proxy to the internal application cluster. They want a cleaner and more flexible solution. My suggestion is to move the VPN to a lower level of the OSI layers. To make the VPN pretty transparent for the user I'll suggest a solution with IPSec, which operate on OSI layer 3. This will harmonize with Saltzer and Schroeder's 8'th design principle, one of my focus. My proposed solution will be like in figure 3. IPSec SW² clients will be installed on the employees laptops. They connect to the IPSec VPN concentrator after the firewall. This means that the firewall must be configured to open UDP port 500 which is used by ISAKMP, the key negotiation protocol used in IPSec. The firewall also must be opened for IP protocol 50 which carries the Authentication Header and IP protocol 51 which carries the Encapsulating Security Payload. With this solution the employees in the customers premises will feel like sitting in the network with the application cluster and can directly telnet to it.

²Software

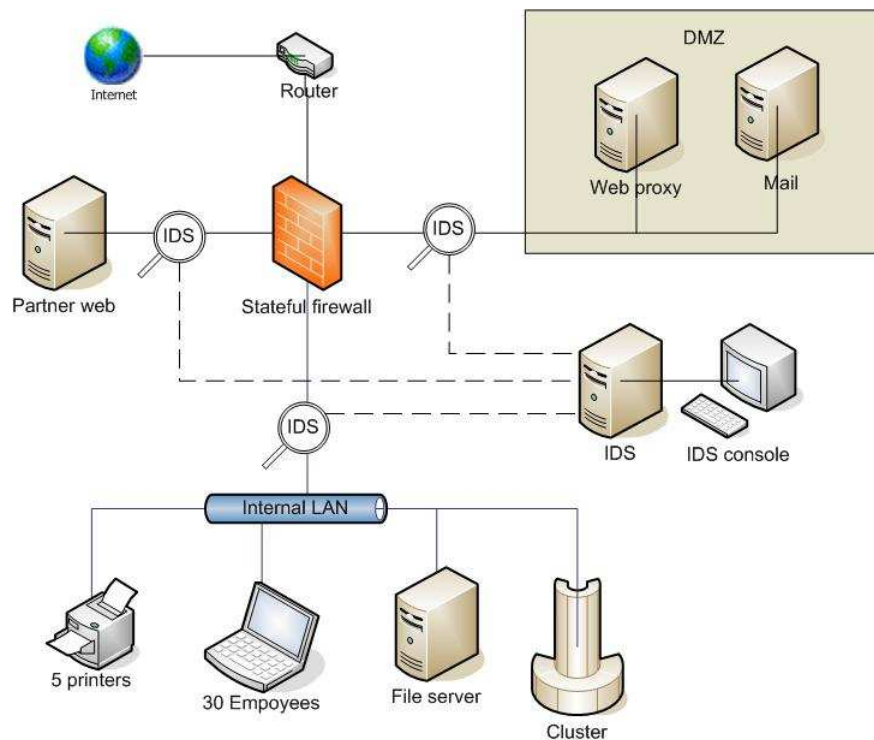


Figure 2: IDS with sensors inserted

5 Personal Firewall

These days it is not enough with just an updated anti virus software. You cannot always trust other computers in the network you are in, or if the network you are in have satisfying perimeter security. There can be many worm-infected computers in the neighborhood. With a strict personal firewall you stop these worms before they enter your computer, independent of your location. Start with the "block all" rule and open ports as they needs to be opened. This will also stop unknown worms and viruses and fulfill Saltzer and Schroeder's 2nd "principle of fail-safe defaults".

In the Windows XP SP2 update there is a bundled firewall, so here is a possibility to save some money on the budget. However, this is not the best firewall at the marked. Some means it is to simple for both the user and a virus to deactivate the firewall. Many commercial firewall like BlackICE and Kaspersky Anti-Hacker also come with bundled IDS/IPS. So a personal IPS software is not needed. I recommend to buy a PFW for all the laptops in FC.

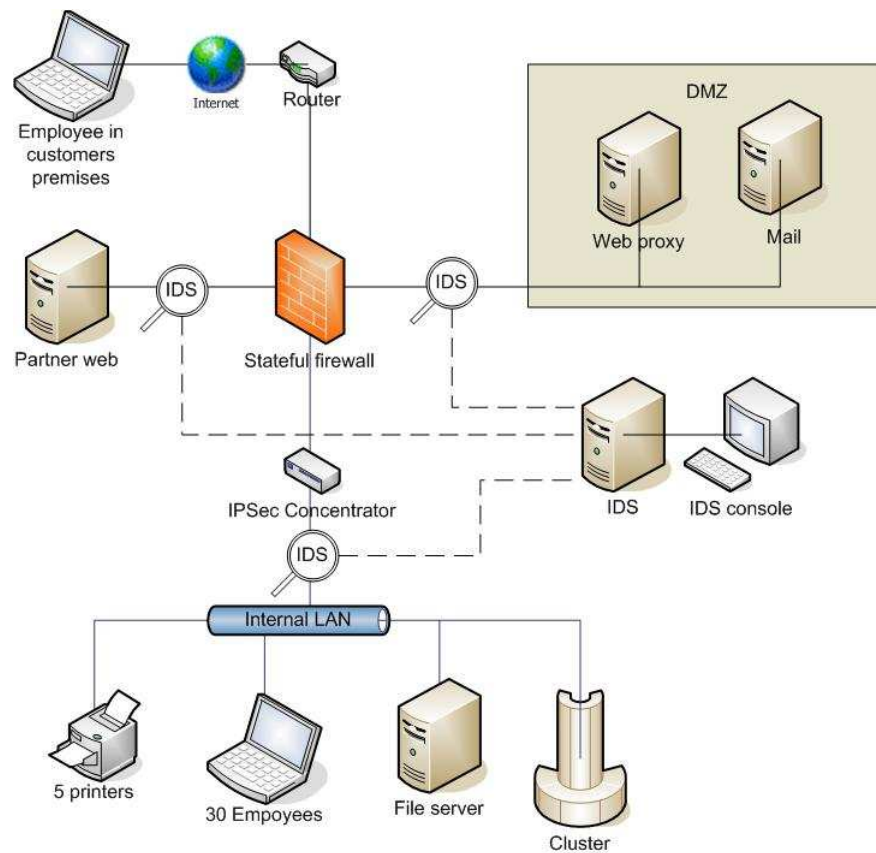


Figure 3: My proposal of the perimeter security

6 TCO

There is often an issue about if the operations should be outsourced to an external company or the company operates itself. There are both pros and cons of both solutions. Some advantages with running the operation inhouse is:

- Control of own environment
- The decisions are made internally
- The know-how stays in house
- Shorter lead time from need to implementation
- May be cheaper than outsourcing (however, the cost are harder to calculate)

The advantages of the inhouse operations is the drawbacks of outsourcing and the other way around. The advantages of outsourcing is:

- Cost usually well defined
- Better access to expertise (hopefully)
- No dependence on key individuals internally

What's the best in this situation depends on the TCO calculations based on the cost table in [Tor04a]. Table 1 and table 2 shows the calculations of the TCO the first year, and the following years. It is calculated with a need of four personnel on each security investment.

	Year 1				Year 2-3		
	Listprice	Training	Wages	Total	SW main.	HW maint.	Total
IDS	125000	40000	160000	325000	12500	6250	18750
IDS Console	45000	35000	80000	160000	2250	35000	37250
30 * PFW	15000	20000	48000	83000	3000	0	3000
IPSec VPN Concentrator	35000	25000	64000	124000	3500	1750	5250
30 * IPSec SW client	0	5000	32000	37000	1500	0	1500
Sum	220000	125000	384000	729000	22750	43000	65750

Table 1: TCO for inhouse operations

	Year 1			Year 2-3
	Implement	Per year	Total	Per year
IDS	27000	108000	135000	108000
IDS Console	Included in IDS	Included in IDS	0	Included in IDS
30 PFW	15000	36000	51000	36000
IPSec VPN Concentrator	12000	48000	60000	48000
30 IPSec SW client	15000	18000	33000	18000
Sum	69000	210000	279000	210000

Table 2: TCO for outsourced operations

As you can see the cost of the first year is lower with outsourced operations. However, the annual cost for the outsourced operations are higher. This means that the outsourced operation will be a cheaper solution in the first years, and after a while the cost will be higher for the outsourced solution. Figure 4 illustrates this example. You see that after four years the TCO is higher for outsourced operations.

These calculations is not accurate enough to take a decision on inhouse or outsourced operations. In the real world there are more factors to consider, as interest, raises in wages, expected price changes etc [Tor04b]. How good the security operations will be is also a difficult issue to deal with. Even though if the solution after some years is cheaper to run the operation inhouse, it may not be so secure as the "experts" would make it. If this results in successful attacks against your company, the price to pay can be rather high.

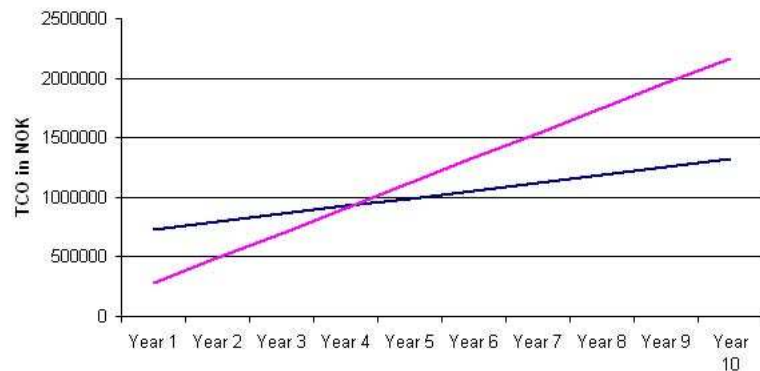


Figure 4: TCO cost for inhouse and outsourced operations

In this case the difference between the inhouse and outsourced operations annually is 144250NOK, and it takes four years before it will be worth inhouse operations. However many things happens in four years. After four years there may be time to invest in new technology and security systems. Therefore I recommend FC to outsource their perimeter security with the solution illustrated in figure 3

References

- [Bis03] Matt Bishop. *Computer Security : art and science*. Pearson Education Inc, 2003.
- [Gol99] Dieter Gollman. *Computer Security*. John Wiley & Sons Ltd, 1999.
- [NWF⁺03] Stephen Northcutt, S. Winters, K. K. Frederick, L. Zeltser, and R. W. Ritchey. *Inside Network Perimeter Security*. Pearson Education, 2003.
- [Tor04a] Espen Torseth. Exercise 3.2 - design case. IMT5061 Perimeter Security, November 2004.
- [Tor04b] Espen Torseth. The principle of tco. IMT5061 Perimeter Security, November 2004.
- [VM02] John Viega and Gary McGraw. *Building secure software*. Addison-Wesley, 2002.