Network Security, Guidelines to Build a Security Perimeter for SMEs

S.Godon and P.S.Dowland

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Network Security is becoming a significant problem for SME administrators. Lack of time, small budget and limited expertise are some of the common issues faced today by most small and medium companies. This paper addresses this problem by proposing a simplified method for securing the network perimeter. Based on the observations made on SME constraints and on the state of the art of current vulnerabilities and threats, this paper presents a decision making approach on how to build a security perimeter for SMEs. Firewalls are obviously the central point of this study. Different guidelines will be provided to efficiently choose a firewall solution.

Keywords

Firewalls, Perimeter, SME

1 Introduction

The great majority of today's small and medium sized companies are dependent on IT systems and most of them need internet access to drive their business. However, the landscape of cyber security threats is becoming more and more complex and now targets companies of any size. (McAfee 2008) Data theft, computer downtime, productivity decrease and loss of reputation are no longer a matter of large corporations. If Small and Medium Companies seems to face the same risks as large companies, they do not have the same expertise and budget to address them. But their principal difficulty is the lack of time to design appropriate security perimeter and manage security issues. This paper presents a method that should help SME administrators to design a security perimeter that fits the needs of the company.

2 Firewall, the key element of security perimeter

A security perimeter is an enforcement zone around the private network to protect the security assets of a company. It is generally composed of many different devices or security services such as anti-virus, content filtering, virtual private networks, intrusion detection systems, authentication servers, vulnerability scanners, etc. However, the foundation of any security perimeter is the firewall. Indeed, the firewall is the entry point of the private network and thus the first line of defence; it creates a barrier (or boundary) between the trusted network (the private network) and the outside (internet) by controlling all the incoming and outgoing traffic. The firewall design is then a milestone to build a good security perimeter.

3 Firewall Selection: a daunting task

Given the key functions of the firewall, its choice is critical for the security of a company. But it is not without difficulties. Choosing the architecture and product that really fits its needs is generally an overwhelming and time-consuming task. The process includes two major phases: the definition of the needs and the evaluation of the different products available on the market.

Prior to the firewall selection, a risk assessment has to be performed to estimate the security needs. This step consists in identifying the critical assets of the company (everything of value to the organisation). It also permits to identify the security weaknesses of the business and thus facilitate the risk prioritisation. However, this step is often bypassed or under-estimated by SMBs: only half of them performed Risk Assessment in 2006 according to the DTI report. (DTI 2006) This generally results in firewall solutions that either under-estimate or over-estimate the needs of the company.

The security needs identified, the evaluation of the available products is the next logical step and not the easiest one. The reason why is because firewalls come up in many different flavours (hardware, software, commercial, open-source), each vendor adding its own buzzwords, proprietary trademarks, adds-on and support contracts.(Taylor 2002; Shinder 2008; Chapple 2005) All this makes the comparison of features not straightforward. If the primary step has not been concluding, it is then easy to get influenced by the firewall offers and purchase a firewall that seems to fit but does not really as long as the company implements it.

The increasing complexity of new threats generally closely related to the constant evolution of new technologies has considerably accelerated the development of firewalls more and more complex to design and maintain. Although SMEs think to save time by purchasing firewall as a one-fit-all product, the result is either at the expense of security or at the one of the business. The principal cause is the lack of time: The McAfee report shows that one third of UK SMEs only spend one hour per week on IT security. (McAfee 2008) In order to address this recurrent problem in SMEs, more support should be given to help them implement and maintain their security system more efficiently.

4 Firewall Design Decision Making (FDDM)

Firewall Design Decision Making is an approach which tends to provide support to SMB in their process of choosing a firewall design that firewall architecture, firewall technologies (or inspection level) and finally firewall products. The method is built in a way to reflect the needs of the company. It relies on key criteria known to be decisive enough to lead to a specific firewall design solution. This method is a questionnaire based approach in 4 easy steps:

- **Step 1** tries to determine the scope of the company and its security objectives.
- **Step 2** intends to determine which firewall architecture best fit the need of the company.
- **Step 3** determines what firewall technology (firewall filter) is the most appropriate.
- **Step 4** investigates which product and features may fit the technical requirements.

4.1 Step 1: The scope of the company

The firewall design is more or less dependent on the specificity of the company: its size, its sector of activity, its geography, the complexity of its network, its personnel, its business objectives...But the most important aspect that conditions the firewall design is the Risk Profile. This latest is what determines the level of protection required by the company. The Risk Profile is the synthesis of three parameters relative to most critical assets: their criticality to the business, their exposure and their probability to be corrupted. These information are the outcome of Risk Assessment, hence the importance to conduct such a process prior to security design.

4.2 Step 2: The firewall architecture

Three main types of firewall architecture exist: The Simple Screening Architecture which consists in one unique box with two interfaces separating the trusted network from the internet, the Multi-Screening Architecture which is one box with more than 2 interfaces which permits to connect networks of different security level, and the Dual Architecture which makes use of two firewalls to separate internal services and external services. The additional zones that are created in the Multi-Screening and Dual Architectures are commonly called DMZ (DeMilitarized Zone). A DMZ is generally a highly secured zone used to provide services to internet users and thus avoid a direct communication between the trusted and untrusted zone.

Although many criteria such as the expertise and time available may enter into consideration while choosing a firewall architecture, FDDM approach uses only the most preponderant criteria:

- The type of services
- The Risk Profile

The firewall Architecture clearly depends on the type of services provided. With internal services only (internet access to internal users), the vector of attacks is somewhat limited, and the choice of the Simple Screening architecture nearly comes in as an evidence. However, if the company decides to open its network to external users such as teleworkers, suppliers, contractors or internet users, the Simple Screening Firewall does not suffice. DMZ(s) should be created to separate the private network from the external services. Multi-Screening or Dual Architecture are the two possible choice. The Risk Profile previously defined should permit to decide between both of them. If set to High, Dual Firewall may best fit the requirement, else a Multi-Screening should be enough.

4.3 Step 3: The firewall technology

There are basically four types of firewall inspection: Packet filtering Inspection, Stateful Inspection, Proxy-level Inspection and Deep Inspection. Firewall products generally use a combination of these technologies to permit more security, however most product fall into a predominant category. The easiest way to tackle the problem is firstly to determine the level of inspection that is at which layer of the OSI model the inspection occurs:

- Packet filtering Inspection and Stateful Inspection occurs at the Network Layer; they basically inspect the header of each IP packet and can filter based on the protocol, source/destination addresses and source/destination ports. First one is static, while the second one keeps track of the state of the connection to deny packets that does not belong to an established session.

- Proxy-level and Deep Inspection filter at the Application Layer; they are able to detect malicious code and viruses contained in the payload of packets. Proxies are the most secure firewall, but they are too specific and slow to fit in all case. Deep Inspection comes then as an alternative combining high security and flexibility.

Two criteria permit to determine which one from the Application inspection or the Network inspection is the most appropriate:

The Firewall Policy

The Firewall Policy is the baseline to implement a firewall solution. It should specify more in details what services should be inspected, why and what measures may apply in case of non respect. Generally, the more precise and complex the policy is, the more probable Application inspection will be needed. And the more dangerous services are, the more appropriate Application inspection will be.

The Risk Profile

The Risk Profile previously determined, provides information about how well the company needs to be secure. High Security Level Business should consider Application Level Filters while Low Security Level may probably get enough from Network Inspection.

Once the inspection level is determined, the choice for the sub-type inspection is a matter of technical requirements. It generally consists in giving priority to one of these parameters: the price, the rapidity or the security.

Hereafter a summary of all firewall inspection:

NETWORK INSPECTION		APPLICATION INSPECTION	
Profile 1 Basic Network Filter - Stateless + Very Fast - Not Flexible - Low security + Cheap	**Profile 2** Basic Network Filter + Stateful + Fast - Not Flexible Medium security + Relatively cheap	**Profile 3** Advanced Filter + Stateful - Slow + Flexible + High Security - Expensive	**Profile 4** Application specific Filter + Stateful - Very Slow - Not Flexible + Very High Security - Expensive

4.4 Step 4: The firewall product and features

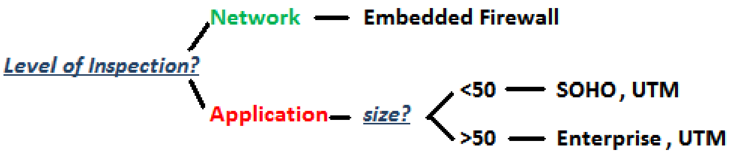
When comes the moment to choose a firewall product, a lot of pending questions still remain. FDDM method focuses on the six preponderant questions. A decision tree generally helps in choosing the appropriate solution.

4.4.1 What type of product to choose?

Products are mainly divided into four categories:

- **Embedded Firewalls**, which are network devices such as router or switches with firewall capabilities.
- **SOHO (Small Office Home Office) Firewalls**, designed to protect relatively small network (up to 50 users).
- **Enterprise Firewalls**, designed for larger companies with advanced monitoring and management needs.
- **Unified threat Management (UTM)**, designed for both SOHO and Enterprise profiles, they protect against the majority of internet threats.

FDDM Method determines which one of the product best is the most appropriate based on the level of inspection (either network or application based) and on the size of the company.



4.4.2 What firewall platform: Hardware or Software?

All firewalls are software running on some kind of hardware, however on the selling market you can either buy a software or an hardware solution. So what are the differences?

Software Firewalls are programs that run on top of an existing operating system (ie Windows, Unix). It can be installed on any existing server in the company but should preferably have its own dedicated machine. The advantage of this solution is that it is usually cheaper at the acquisition and scalable (or expandable) to meet the future requirements of the network. The downside however, is that they are more prone to hardware failure, are vulnerable to OS attacks and are difficult to maintain since this solution supposes to keep up to date the OS system as well as the firewall software.

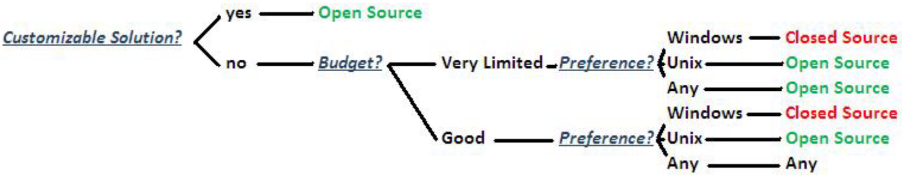
Hardware Firewalls are programs that run on dedicated devices specifically designed for the purpose of firewalls. Hardware Firewalls provide a great advantage over software based solutions. Also called turn-key solution, they are plug and play devices, easy to use and maintain with no need to secure the underlying operating system. Furthermore, they contain only what they need to run compared to computer-based solution composed of many more components subject to many more failures. The constructor warranties and the following up of products and bugs make Hardware Firewalls more reliable than computer often home-made. The downside of firewall box however is its cost and its lack of upgradability. If the future growth of the company is not taken into account during the choice of the appliance, this one will probably not fit the future needs.

4.4.3 Free or Commercial Software?

While Hardware solution will always be commercial solutions, Software solutions can be either commercial or free. When choosing between both of them, the best thing to do is probably to assess the overall cost, the features and the support available. The pitfall would consist to believe that because a solution is free, it is the most cost effective solution. However, the cost of implementation and maintenance could reverse the balance. No general decision tree is provided in this case, because of the variety of products. Indeed, free firewalls can outstrip some commercial products.

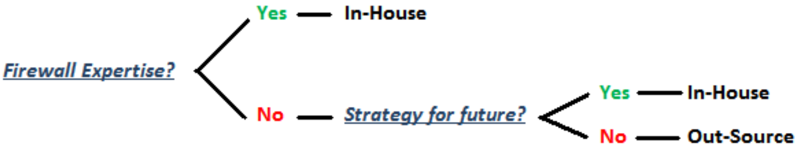
4.4.4 Open Source or Closed Source?

There is often a misconception that Open-Source means Free of charge, but it is not true. Open Source can be the basis for commercial products. Some of the examples are Untangle, Vyatta, Sourcefire, which are all commercial Firewalls built on Open-source architecture (Directorym.net 2008) Open-Source means the source code is available in clear to anyone who wants it. By contrast, Closed-Source or Proprietary Software keeps their code secret to the end-user. It may be tempting to ask the question “Which one of them is the most secure”. However, this is probably the wrong way to tackle the problem. The right way is probably to know how flexible the solution must be and how confident you are in both strategies. The decision tree implemented in FDDM is as follow:



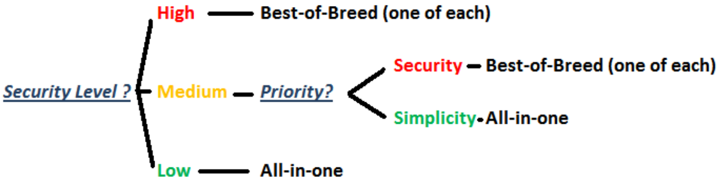
4.4.5 In-house or Out-Source?

Firewalls are just as secure as you tell them to be. In other words, a good firewall will not provide good security if it is not well configured. Firewall configuration and maintenance is not an easy task and requires competencies and experiences. The choice to leave this task to an experimented third party could be an alternative for small and medium companies with no in-house expertise. It permits to get rid of the firewall configuration, administration and maintenance. However it does not exempt the company to define the firewall policy to apply and to check that the outsourcing company complies with the term of the policy. Although tempting, outsourcing generally offer limited services and may not be as flexible a solution as managing itself the firewall. Furthermore, this option implies to trust the out-sourcing company, not a viable option for anybody. While assessing the need for outsourcing or not the firewall, one should ask the following questions: Do you have firewall expertise in-house to ensure the maintenance and administration of the firewall? Is that part of the strategy of the company to develop firewall expertise?



4.4.6 Best-of-Breed or All-in-one?

Since the apparition of UTMs, numbers of debates oppose partisans of Best-of-Breed solutions and partisans of All-in-one solutions. The Best-of-Breed configuration consists in implementing the best of each security products with the idea to create several layers of protection: in other words, it means buying a firewall as a first line of defence, buying a separate anti-virus as a second one, buying a separate anti-spam, a separate intrusion prevention system and any other security device depending on the level of security needed. By opposition, All-in-one solution which best example is probably the UTM, is a concentrate of all the security devices in one unique box. The immediate advantage is the reduced price and the easy management of the security. The downside however is the lack of defence-in-depth with one unique point of failure.



5 Conclusion

The evolution of technologies went with a multiplication of threats more and more difficult to manage. Securing the perimeter stays one of the best practises to keep away attackers. However, as threats have become more sophisticated, perimeter solution also became more difficult to design and maintain. Firewalls are one of the best examples. The principal victims of all this are Small and Medium Companies for which the factor time and budget does not permit to efficiently respond these security issues. This paper has described some of the outcome of the Firewall Design Decision Making (FDDM). This methodology, although not already tested, intends to help SMEs in choosing more efficiently a firewall solution that fits their needs. FDDM should save time to administrator since it has solution oriented approach. However, one should also understand the limits of this approach. FDDM is an help to the firewall decision, but not for its implementation. No matter how good is the firewall if bad is the implementation. Furthermore, this study focused on securing the perimeter while most of the recent threats may come from the internal network. It is clear that the protection of the perimeter is not the only security challenge that face Small and Medium Companies, nevertheless any singe contribution can help to make security more affordable for SMEs.

6 References

Chapple, M. (2005). “How to choose a firewall”. SearchSecurity.com. http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1113533,00.html, (Accessed 12 January 2008)

Directorym.net (2008) “Open source security: 10 commercial vendors”. http://articles.directorym.net/Open_Source_Security_10_Commercial_Vendors-a899079.html, (Accessed 14 June 2008)

DTI (2006). Information security breaches survey. http://www.enisa.europa.eu/doc/pdf/studies/dtiisbs2006.pdf, (Accessed 12 December 2007)

McAfee (2008). “Does size matter? The security challenge of the smb”. http://www.mcafee.com/us/local_content/reports/does_size_matter_en_v2.pdf, (Accessed 15 August 2008)

Shinder, D. (2008). “Choosing a firewall”. WindowsNetworking.com. http://www.windowsnetworking.com/articles_tutorials/Choosing_a_Firewall.html, (Accessed 15 February 2008)

Taylor, L. (2002). How to choose the right enterprise firewall. ITmanagement.earthweb.com. http://itmanagement.earthweb.com/secu/article.php/974501, (Accessed 15 February 2008)