Global Information Assurance Certification Paper

Concepts of Perimeters Design

SANS GSEC certification
Practical Assignment version 1.4c – Option 1
SANS Ottawa Parliament Hill August 2004

Marc-André Frigon

18 January 2005

Abstract

Perimeters design is a complex and wide area of computer and network security. The scope of this paper is to overview concepts to keep in mind when performing the high level design of an organization boundaries protection. Physical security, requirements definition (technical, risk assessment, assets classification, etc.), definitions of organizational security policies and understand the organizations practices as well as the implementation the design are all beyond the scope of this paper. The underlying intent of this paper is focus on the general hints to achieve a secure design of organizations perimeters.

Perimeters are not anymore limited to network end point, they are brought to the application layer, to the data itself, to the user education, to content filtering; which impose to the perimeters to address all those needs and include monitoring, trending, alarming solutions as well as the appropriate enforcement mechanisms to ensure the availability, the confidentiality and the integrity of the organization's resources. Securing the perimeters means making the whole system coherent with its subsection, it means creating strength throughout the organization infrastructures and support more efficiently the business needs. With the concept of In-Depth Defense in mind during the design process, the result is more likely to stop or to significantly slow down unexpected activities to damage the organization.

Table of contents

1 Define the Perimeters & the Security Needs 1
2 Perimeter design principles 2
2.1 Reduce the number of in/out points 2
2.2 Choice of the Appropriate Technologies to Segregate the Different Level of Security Segments of an Organization 3
2.2.1 Network elements 3
2.2.2 Application aware devices 4
2.2.3 Applications payload inspection 4
2.2.4 Access Control 5
2.2.5 Monitoring, Alarming and Trending 6
2.3 A Secure Design does not Rely on a Single Product or Technology 6
3 How to Protect the Boundaries 7
3.1 In-Depth security model – layering 7
3.2 Security from layer 1 to 7 of OSI model 8
3.2.1 Border router ingress and egress filtering 9
3.2.2 Stateful packet inspection firewall 10
3.2.3 Application aware firewalls 10
3.2.4 Add-on to the application aware firewalls 11
3.2.5 Monitoring 11
4 Put Everything Together 12
5 List of References 13

List of figures

Figure 1 - Onion model of Defense 8
Figure 2 - Network Model 9

2 Define the Perimeters & the Security Needs

The latest trend in network security is to talk about the de-perimeterization of network, which mean that due to the current business needs (more traffic need to be allowed to cross the borders) the traditional perimeters are becoming more and more porous. The perimeter security is becoming a matter of enforcing security not only at the external borders but also in the inner section of the network as well as up to the application layer for all computer and network resources.

> You may recall the Twinkie analogy for network security: hard on the outside, soft and gooey on the inside. This is the old method of securing the network; it's a model that frankly no longer applies as new exploits have been released. This method frequently overlooks what we ultimately try to protect -- the data.[1]

The best security practice in perimeter implementation is to segregate different level of security environment (with appropriate device(s)) and to limit the interaction with the least privilege concept (allow only what need to be allowed and nothing more). The organization boundaries are not limited to the Internet access and/or some links (facilities) with partners and/or partners. Perimeters should also exist within the organization internal network to segregate the different subset of the organization that are not in the same security trust level; and even some segregation between the same level of security subset should exist in order to keep the segregation feasible (the administrator(s) has to understand the traffic and manage the filtering).

Perimeter security is not a matter of product, it is a process that has to become part of the business practice; it has to become part of the accepted practices not only posted on an internal web site or shown once a wile to the external security auditors. In order to ensure a good security level between different level of trust subsets of the organization, the proper choice of product has to be made based on the particular needs.[2] It is mandatory to implement security enforcement point(s) up to the appropriate level of expected segregation and security level. Not all segregation has to be enforced up to the application layer, but this decision of the level of segregation as to be taken based on the design and security requirements. Often forgotten in perimeter design, the physical security is the first thing to look at of before thinking about nice and fancy enforcement mechanisms (someone may have the tightest firewall policy with the more secure product ever made, if everyone has physical access to your boxes, it does worth much more than “nothing”) – NOTE: the principles of

---

[1] Noonan, Wes. 20 September 2004

[2] Cisco Systems. Internetworking Technology Handbook - Security Technologies

physical security are not treated in this paper.

It is mandatory to impose a stronger security mechanism to the weaker element of the company computer resources; let say the company has an old system that is not anymore supported by the manufacturer and that cannot be upgraded or migrated to something else and even more that service is mission critical for the enterprise, then for sure the security enforcement has to be more important (tighter) then for other element of the enterprise. This could mean enforcing security up to application layer for an internal web server (reverse proxy) even if the first impression this solution might appear as too extreme. The concept to remember is that the security of the whole corporation is as strong as the weakest security point; it is mandatory to identify the weakest points and to efficiently work to improve the security of those points to strength the whole system.

3 Perimeter design principles

Previously in the design process (not treated in the current paper), the segregation points (choke points) and required level of security segregation as well as some technical design requirements (e.g. does the organization runs open source software in its production environment?) were stated. With all those requirements and decision in mind, the next topic to focus on, for designing a good perimeter security system, is to overview the security best practices for perimeter design. The most important things to keep in mind when designing the technical security enforcement of organization perimeters are:

- Reduce the number of in/out points;
- Choice of the Appropriate Technologies to Segregate the Different Level of Security Segments of an Organization;
- A Secure Design does not Rely on a Single Product or Technology.

3.1 Reduce the number of in/out points

Keep the number of interconnection points between networks to its minimum. Which lead to minimizing the number of network security devices to deploy, to manage and to maintain. Some organizations spread the Internet access in 2 entities to segregate the internal traffic to the Internet (may also include traffic from and to business partners and customers) from the Internet traffic to the public services offered on the Internet (may also include traffic from and to business partners and customers). The major concern here is to limit the number of external point of presence to its minimum to force all the traffic to cross the same security devices. With today business needs, the security policies are porous to support the more and more open environment; by limiting the number of point of presence you ensure a minimum number of points to monitor and focus the administrators' attention to the most relevant information

and to capture evidences.

It is definitively recommended to hook the remote access services (RAS) such as VPN boxes and modem pool to an external firewall to filter the incoming traffic from those external networks. By such practice, the security level of the protected systems is not decreased to the level of the "external" remote system. Hint – do not assume or rely on others to ensure your own security.

Keep in mind that limiting the number of interconnection points means limiting the number of filtering devices. Filtering devices are good as long as the traffic hit them (a little limitation no!), position your filtering devices at those location.

3.2 Choice of the Appropriate Technologies to Segregate the Different Level of Security Segments of an Organization

3.2.1 Network elements

It is now an industry de-facto standard to use at least a packet filtering device to protect against the Internet traffic, but this choice of technology does not apply to every choke point like the ultimate solution of every case. Many network devices are used to ensure an appropriate level of security (switches, routers, Stateful Packet-Inspection Firewalls).

A generally recognized as a good practice is to segregate in different the end users subnets from the servers they need to access (e.g. file servers, mail server and internal web page) and to mitigate the risk of hazardous (malicious activities, users errors or worm propagation) the use of the existing infrastructure with ACL is cheap, efficient and it does the job[3]. That recommendation would certainly not apply to an internal segregation between HR or R&D or accounting servers and the rest of the company, but it does hold the road for not high value and priority company's assets.

For stronger security requirements, a Stateful Packet-Inspection Firewalls is the standard tool. In brief, it does not only base its decisions on either the source or the destination IP address or the service, but it keep track of the logical sequence of the communication (e.g. it enforces the fact that TCP tree way hand-shaking is required for establishing a TCP connection), some of the more advanced products will reassemble fragmented packets before allowing them communication to occur. Many products are available on the market, but in brief those devices are expert to analyze the traffic and challenge the validity of the packets up to layer 4 of the OSI model. Their usage is normally reserved for interconnection between untrusted (external) networks and trusted or half-trusted networks.

[3] Deterding, Brent. "Segmenting Networks: ACLs"

The actual trend in the firewall and IDS/IPS markets is to offer transparent bridge mode devices, these devices are "transparent" from the rest of the network and can drop (the drop packet vanishes), reject (with Reset flag for TCP connection or ICMP port unreachable for UDP sessions) or accept based on some criteria. The interest for such technology resides in the fact that they are invisible, which make them good friends for the computer and network security community; they their nature these devices are stealth which make them hard to find for mal-intended people). Depending of the chosen product, they can be used in passive mode (monitor and alarm) or in active mode (quarantine a host or a subnet or act as an active countermeasure to attacks).

3.2.2 Application aware devices

Application aware firewalls, also known as application proxy firewalls or application gateways are specialized products to enforce security measures from layer 5 to 7 of the OSI model. Their strength is to be aware of the application (which is usually considered as the payload for the network elements), they allow the communication to take place only if it respect the security policy which dig into the upper layer of the OSI model.

An application proxy firewall may address the needs for Internet usage from the internal network, it would allow an organization to stay (or to become) a good Internet neighbor by ensuring your people are not sending "garbage" on the net. This technology also allows the security team to enforce the security policies concerning the Internet usage from the office (no pornographic sites, no racial discrimination, no political propaganda …) through content scrubbing. An other major advantage is that usually the application proxy firewall can cache the content which may reduce the Internet connection usage. The caching concept is such that the first user that tries connect to a web site, the proxy load the page for the user and sends it back to the requester, then and other user request the same page the content is sent to the second requester without leaving the organization network.

Application gateways are also to protect a corporation servers, it is mostly refer as reverse proxy because they aggregate the request from many source to one destination. Again the main purpose of such implementation is to protect the organization resources (application servers) against undesired communication, but mostly in the upper layers of the OSI model. Some reverse-proxies offer the caching capability such that they may improve the service performance in the case the content is relatively static.

3.2.3 Applications payload inspection

Above the RFCs and protocols guidelines, the content of the communication might be also filtered based on an organization's security policies. Content scrubbing can be done in different fashions such as a firewall

(no matter which technology) requesting a content sanity check to a specialized product or in an application aware firewall itself (I personally believe, in general, that a specialized device is more likely to perform a better job then a box that does everything).

Often, emails header posted on news group are good source of information for bad intended mind, telling then the smtp product running within an organization. In order to prevent such information "leakage", it is a good practice to implement a smtp-relay (known on the Internet has the domain MX record) that strips the good information from the email headers[4] and it could also enforce the anti-virus check as well as the content scrubbing base on the organization security policies. For most people, the most annoying malicious activity on the Internet is spam (no needs to give more details) – to prevent an organization to be a victim of such activity it is mandatory to implement anti-spam devices and an smtp-relay is the best location to perform such activity. The anti-spam inspection should also scan the outgoing email to prevent the organization to send unsolicited emails and obviously the mail-relay server is not an open relay for the rest of the planet. Emails are good carrier to spread virus, any organizations should filter the emails' attachments for virus presence (it does not mean the other resources should not run Anti-Virus) – it may save a lot of troubles.

3.2.4 Access Control

A major consideration in security (not only in computer and network security) is access control. Think about it, in order to take a flight you need to pick your boarding pass (with a picture ID), then cross the airport security, then, if you are lucky you will only show your boarding pass before have access to the airplane, if you are not they might ask you again for your IDs. The same concept applies to computer and network security, before accessing an organization resources, one should be challenged for its identity.

With the actual business needs of mobility and partnership, most organization needs to implement remote access systems such as VPN or dial up systems to sustain the interaction between remote employees and partners to its internal network and resources. In order to efficiently address those needs, implementing strong authentication (at least 2 way factors authentication) is the industry de-facto standard for remote access to an organization facilities. Keep in mind that some malicious people will try to brute force your remote access devices, so monitor the authentication attempts. Since the remote access are usually deployed for accessing the organization internal resources, it is strongly recommended to implement accounting services on the RAS and also on the accessed systems to keep evidences of the activities.

---

[4] Brenton, Tack 2 - p. 28

3.2.5 Monitoring, Alarming and Trending

Knowing your network and knowing your traffic is one of the most forgotten field in computer and network security. Knowing who talks to whom, for how long, how often, on which service, to which application, what is the data transfer rate and so on would help quite a lot to prevent and alarm unexpected events (DOS or DDOS or password brute force or etc.). Once you have good monitoring and alarming mechanisms in place for the most critical points of the organization network and you have enough information and knowledge of the "normal" situation, it might become interesting the implement limitations mechanisms. The limitation may be done on network element for priority queuing (most application like VoIP are more susceptible to network latency than emails). Bandwidth limitation can be enforced to protect your asset, let's say 30 percent of the Internet traffic to your public services is http/https to your web servers – why don't you limit the usage to up to 50 percent (those values are only indications), such that if someone tries to flood you Internet connection, the risk is mitigated. The same logic may apply the number of request per minute or second from one source IP address or to one destination to limit the connection rate and/or total amount of connections. The logic here is to understand what is normal and to make sure things are staying normal by limiting the activity to an acceptable level. Be careful when implementation such limitations, you might shoot yourself in the foot if you don't understand your traffic and network as well as the chosen enforcement mechanism (it is a good practice to test it in a none production environment first). SNMP and RMON pooling are good and cheap way to learn, to monitor and alarm the network activities; the retrieved information can be used to perform trending analysis which may lead to a continuous improvement of an organization network.

With the industry trend to implement self-teaching devices, such as IDS/IPS, that learn what is normal instead of matching all the traffic to predefined signatures (evidences known as malicious activities) the security administrator job might become easier – I personality would not rely exclusively in such product for monitoring the network activity but I use it with other tools.

3.3 A Secure Design does not Rely on a Single Product or Technology

It is largely known and accepted that all products are vulnerable to some security breaches (commercial and open source products) and yes! even the security enforcement product fall in this category. The fact is that the products are becoming huge and errors or misinterpretation of the standards are induced weakness in the code (larger the code is, greater are the chances that an "error" will happen). In order to mitigate the risk of running vulnerable software in an organization environment, it is a security best practice to use a variety of

products in its deployment and mostly for protections that are in series such as firewalls. Patch management and keeping the running software to an up to date version will help to mitigate the risk associate to the product. Even with good patch and software management, if all your security devices are running the same release and the vulnerability is known and no patch are yet released, then you are most likely susceptible to be an easy prey for malicious activity. It is always a matter of time to figure the weakness of the available product, no matter if it is open source or commercial products.

Learn about the product you deploy, challenge their behavior, and understand their strength and weakness. It might sound ridiculous, but not all products are good for the same usage (even if they claim to). Knowing the limitations of the products an organization is planning to deploy leads to better choices to improve the security level.

User education should be part of your perimeters design; no matter how strong are your design and implementation, if the information and resources are not protected by the organization people. Remember that a firewall can only filter the traffic that cross it, this is the best image to demonstrate that an employee can print on paper or burn on CD-ROM and carry out this important information out of the office or if your users are sending by email (neither encrypted nor signed) critical information over the Internet. Not only an organization should teach their employee, partners and customer about security, they should limit the access to want the employee need to have access for their normal function (not more and not least then what is required).

4 How to Protect the Boundaries

4.1 In-Depth security model – layering

With the concept of in-depth security, apply the onion skin model in your design. In this model, the most external layer are refer to untrusted environment surrounding your own organization – e.g. Internet, business partners & customers thru dedicated links or VPN tunnels or physical access (are you aware of their security practices? Did you audit their security? Do you schedule to do so?) and deeper in the inner circle are residing your most valuable assets (customers confidential information, R&D, financial and HR information). By applying layers above layer of security tools, you enforce the in-depth security principle[5]. The security level classification and segregation are not treated in this paper; it is assumed that is provided in the previous steps of the perimeter design based on the requirements and on the organization's security policies.

[5] Braggs, Roberta, Marck Rhodes-Ousley, and Keith Strassberg. p. 39

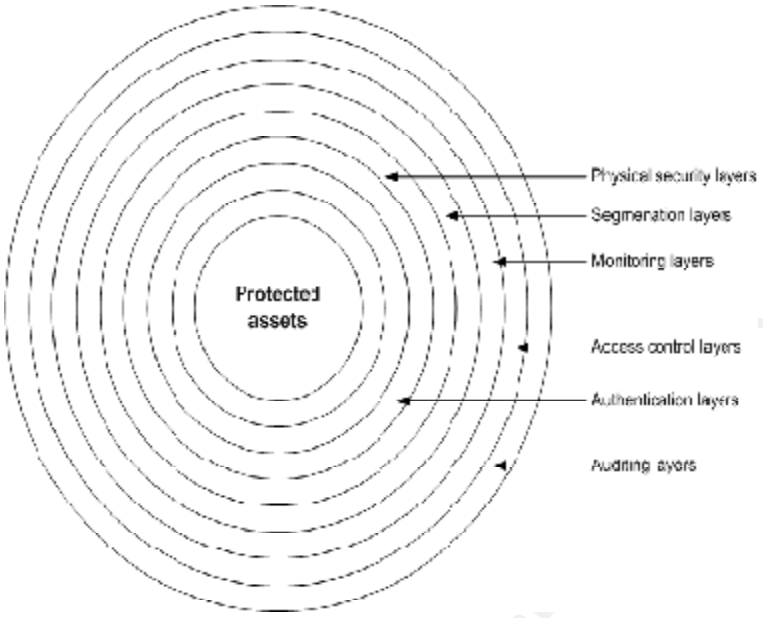

Figure 1 - Onion model of Defense

Layering of products in series is an art, the designer will have to determine how to integrate each one with the others in order to improve the security level and to keep or better improve the performance of the whole system. Based on the OSI model and with the in-depth security principal in mind, it is mandatory to protect organizational assets from layer 1 to 7; the desired level of security to implement should be state prior to determine the way to implement the perimeter protection.

4.2 Security from layer 1 to 7 of OSI model

It is normally accepted that services that are Internet accessible and important for an organization are most likely to request the highest level of security. Based on that assumption, some conceptual descriptions of what to do and how to do them are presented. In order to enforce the in-depth security principal, an up to layer 7 of the OSI model should be implemented (since the scope of this paper does not include physical security, it is assumed that the logical protection is coherent with the physical security). Addressing security for layer 2 of the OSI model is made with VLAN usage and enforcing a layer 2 protection on the switch device[6] – it is common to use different switches for different level of security VLAN (segregation of layer 2 equipment based on the security level of the use for subnets). Since most product on the market are made to protect layer 3 and 4 as one set of rulebase (layer 3 and 4 filtering functions are aggregated in one security policy), it is recommended to perform ingress and egress filtering on the border router and to couple this filtering mechanism with a stateful packet inspection firewall (a device that will inspect

[6] Vyncke - Ethernet: Layer 2 Security

all packets and keep track of what is expected and what is not up to layer 4). To protect from layer 5 to 7 of the OSI model, an application proxy firewall per service basis will protect up to the application layer from unauthorized usage and this proxy firewall may rely on an other security devices that will ensure the "quality" of the content (web content scrubbing, virus scan, http tunneling, etc.). In order to implement good and efficient perimeter design, it is assumed that the organization is using internal IP address scheme for internal usage and public IP address only for external services – it is cheaper and it adds an other security mechanism to the enterprise environment. The picture below may represent an overview of this design.

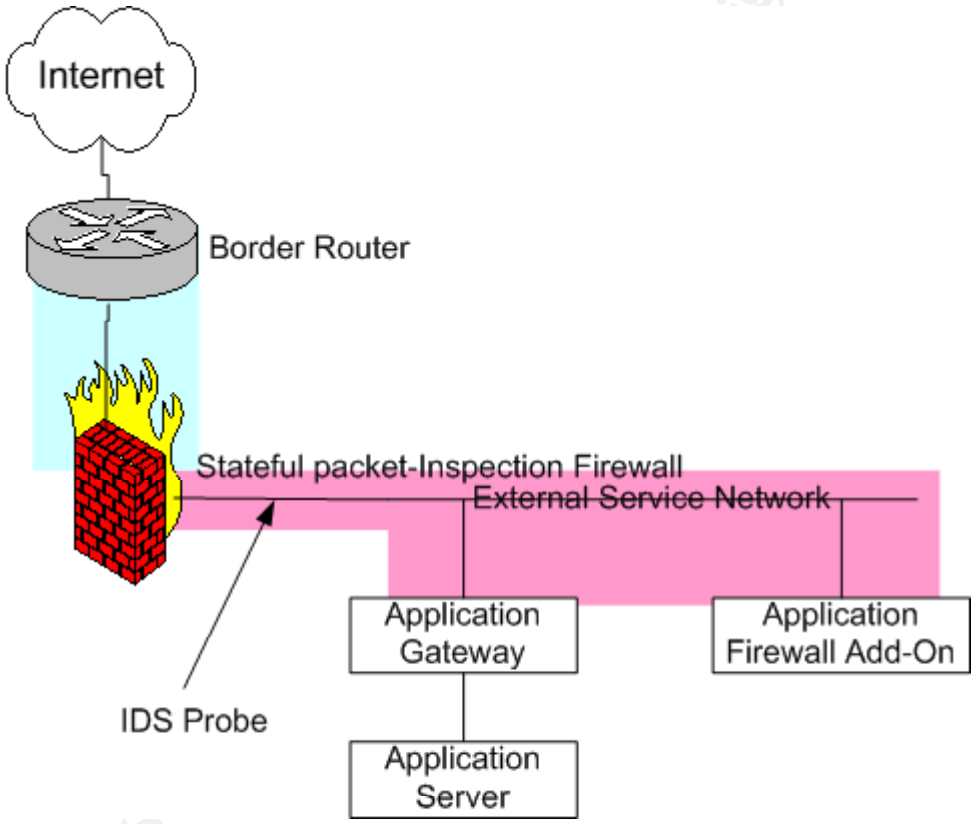

Figure 2 - Network Model

4.2.1 Border router ingress and egress filtering

In terms of security, the border router is used to protect the network against traffic that cannot be legitimate or that is surely undesired (based on the SANS TOP 20 vulnerabilities[7], source based routing, spoofed traffic and more) and also to protect the network against banned sources such as known attacker IP addresses. The second major security concern with the border router is to unload the external firewall (since the border router drop certain traffic, it leaves more of the external firewall power to deliver faster inspection of the remaining traffic). The usage of ACL (Access Control List) is made in both direction

[7] http://www.sans.org/top20

incoming as well outgoing traffic (ingress and egress), to protect some leakage in the statefull packet inspection firewall (un-nated packet going to the Internet). In order to implement a good implementation of this ACL, many sources are widely available[8].

4.2.2 Stateful packet inspection firewall

As shown in Figure 2 - Network Model, the stateful packet filtering firewall is the central node of security filtering at an organization boundary; it is one of the most important security enforcement mechanisms and a good understanding of the product strength, weakness and limitation is mandatory for achieving a good design. In the presented model, the stateful packet firewall node enforces up to the layer 4 of the OSI model (usually layer 3 and 4) the security of most of perimeter design. Its primary role is to deeply inspect the connections and filter the undesired and unexpected packets (e.g. the firewall will keep track of the TCP sequence and acknowledgement number to figure if the packets are really part of the active connection and/or is will only allow TCP packet with only a SYN flag on and nothing else as the first packet for establishing a TCP connection). The firewall itself is protected by the border router and does protect the internal resources of the organization.

When designing an organization perimeter, it is important to figure where are the gate keepers (the performance limitation points in the design) to scale properly the boxes and to address the network performance requirements. The same principal applies to the security concerns, which level of security you want for a particular application or server? Since the stateful inspection firewall is most likely a major network and security node in the perimeter design and in both domains (network performance and security enforcement) the strength of the whole system is as strong as the weakest portion of it (both speed and quality of inspection).

The usage of stateful packet inspection firewall is mostly recommended for segregate different level of trust subset of an organization (e.g. Internet and screened network – untrust to trust networks). It is accepted among the security community that almost every organization should implement at least a stateful packet inspection firewall between any level of trust and an untrust environmemt (e.g. Internet, most business partners and clients, etc.)

4.2.3 Application aware firewalls

As mentioned earlier, most of the security above layer 5 of the OSI model is spread between the firewalls that are application aware and specialized products. This implementation improves the security of the whole architecture, provides a Defense-in-Depth model to the network (reduction of the dependency

[8] Deterding, Brent. "Segmenting Networks: ACLs"

on one single security device) and allows more tuned and precise configuration for the specific needs of each service and/or server.

By enforcing the security of the perimeters up to layer 7 with such firewalls, the chances that undesired or expected traffic hit the application servers are greatly limited to its minimum (so, unlikely to happen – which represent the desired behavior). In fact those devices are inspecting only (or mostly) the content of layer 5 to 7 of the OSI model to challenge the validity of the packet payload and to allow through only the expected traffic – this could mean for an FTP application to allow *get (and mget)* command and refuse *put* (and *mput*) command.

The application proxy firewalls are known to be highly CPU intensive under heavy load and very specialized products in terms of scope; which explains why it is recommended to use then on a per dedicated service basis or per server basis with the proper performance scaling.

4.1.4 Add-on to the application aware firewalls

Since perimeter threats are not anymore limited to the 7 layers OSI model, but also to the content of the application layer (e.g. SPAM or web content scrubbing), some specialized security devices are available to protect the "quality" of the content at the application layer (web content scrubbing, virus scan, http tunneling, etc.). Keep in mind in the design phase that an organization is accountable of its members' actions and it may save a lot money and time to appropriately filter the content of applications. The security policies of any organization should include such prevention. No organization to be known as a bad Internet neighbor that spreads virus and worms across other networks (mostly antivirus software protection will address those issues)? Is it normal and desired to let the members of an enterprise consult not related to their task offending web site (pornography, terrorism, hacking techniques and so on)? Web content scrubbing and ads ripper are available to protect your organization against those undesired behaviors.

4.1.5 Monitoring

In order to well manage the organization perimeters, it is mandatory to understand and track the traffic (from layer 1 to 7). IDS/IPS (out-of-band or in bridge mode) probes are good to perform this task; looking and capturing evidences of attacks (attempts or successful). SNMP/RMON pooling to the border router, the packet stateful-inspection firewall and the application servers as well (for proper values) will increase the administrator(s) awareness of the activity leading to enforcing the appropriate threshold levels. Gathering the information should be included in the perimeter design and analyzing the data should always be an on-going process to improve the validity of the configuration.

5 Put Everything Together

Now that the designer has a global vision of the security mechanisms in mind and he/she has a good understanding of the requirements (security, performance, organization practices and more), it is time to build a coherent assemblage of tools. Putting everything together is an art that is beyond the scope of this paper (product choices, configuration considerations, implementation compromises and many other facts of live). The design process should also include a feedback loop to challenge initial requirements and the proposed solutions to address them. The same feedback loop should be present between the design on paper and the implementation, which mean that not only the implemented design should be analyzed for its implementation configuration but also audited (sooner or later someone will do it … why don't you challenge yourself first).

6 List of References

Braggs, Roberta, Marck Rhodes-Ousley, and Keith Strassberg. Network Security – The Complete Reference. Emerville: McGraw-Hill/Osborn, 2004.

Brenton, Chris. Track 2 – Firewall, Perimeter Protection, and Virtual Private Networks. Volume 2.2. SANS Press, 2003.

Brenton, Chris. " What is Egress Filtering and How Can I Implement It?". SANS Reading Room. 29 February 2000. <http://www.sans.org/rr/whitepapers/firewalls/1059.php>

Chapman, D. Brent, Simon Cooper, and Elizabeth D. Zwicky. Building Internet Firewall – Second edition. Cambridge: O'Reilly & Associates, 2000.

Deterding, Brent. "Segmenting Networks: ACLs". SANS Webcasts. 1 July 2004. <https://www.sans.org/webcasts/show.php?webcastid=90512>

Cisco Systems. Internetworking Technology Handbook - Security Technologies. 20 February 2002. <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/security.htm>

"Firewall White Paper - What different types of firewalls are there?." Vicomsoft. 2003. <http://www.firewall-software.com/firewall_faqs/types_of_firewall.html>

"First Things First - An Introduction to Learning About Network Security." SANS –Internet Strom Center. <http://isc.sans.org/presentations/first_things_first.php>

Kumar, Rajeev "Firewalling HTTP traffic using reverse squid proxy." SysAdmin. Feb 2004. <http://www.samag.com/documents/s=9023/sam0402c/0402c.htm (20 February 2004)>

Newman, Glenn and Steve Weil. "Firewalls - Strategic and Technical Considerations". Seitel Leeds & Associates. 13 February 2003. <http://www.sla.com/html/links_pubs_files/UserGroup2.PDF>

Noonan, Wes. "The weakened state of the network perimeter." Windows Security News. 20 September 2004 <http://searchwindowssecurity.techtarget.com/originalContent/0,289142,sid45_gci1007026,00.html>

*Ruest, Danielle and Nelson Ruest. "*Serious Perimeter Security - Use these two keywords to make your perimeter more secure." FTPOnline.com. 1 November 2004. <http://www.ftponline.com/special/security/ruest2/>

Vyncke, Eric. Ethernet: Layer 2 Security. Cisco Systems. 2003. <http://www.terena.nl/conferences/tnc2003/programme/slides/s1c3.pdf >

Welch-Abernaty, Dameon D. Essiential Check Point Firewall-1 NG. Boston: Addison Wesly, 2004.