



Securing your perimeter isn't just about keeping people out ... but also keeping them in

What is your perimeter?

In the early days defining your perimeter was easy. The perimeter consisted of your castle. Security consisted of a moat with drawbridge, high walls with guards stationed on top. When a visitor wanted entry he was announced and the landlord decided if he could enter or not.

The early networks had a similar setup. The perimeter was your network and the firewall your perimeter defence. The rules set on the box defined whether or not a connection could enter the perimeter. Since no intelligence was added another rule set defined what connections could get out. The stateless firewall was born.

So ... what is your perimeter? ... Is it the data centre that hosts your servers? Is it the buildings where your employees have their desk? Should you consider the Wireless Network your using as a part of the perimeter or as a threat? Mobile devices travelling around are constantly accessing your network swapping out data. Are they outside your perimeter or should you consider them part of it?

Once your perimeter defined the challenge gets really started: how will you secure it?

What can we do for you?

Today securing your perimeter is a lot more than just dropping a few boxes between the outside world and your network. Scalability, throughput, proper designs have to be envisioned. There are many brands and technologies but do they all serve your needs?

As a leading consultancy and vendor-independent company Ascure specializes in Operational Risk management. As such we can help you and your organization independent of brand or solution so we can strive to the benefit of your organization. And we can do this throughout all stages of your ICT security projects.

About Ascure

Ascure is specialized in operational risk management consultancy and staffing. Operational risk management, information security, business continuity and compliance to laws and regulations are major cornerstones of our services.

Ascure assists its customers with the incorporation of operational risk management at all levels and in all areas of their organization, including day-to-day operational decisions. No decision should be taken in any organization without applying proper operational risk management. It can be applied throughout the entire life cycle of any activity or project. In order to minimize risk, it is however preferable to apply operational risk management at the beginning phase of a project or operational activity.

About Ascure Academy

Ascure offers, through the Ascure Academy, an extensive education and awareness program, covering several open classes, events and customized education experiences.

Contact

For further and additional information, please contact us on Tel. +32 (0)9 243 10 20 or info@ascure.com

On all Ascure services our general terms of delivery apply.

Mapping your business needs

When starting IT Security within your organization it is important to know the needs your organization has as well as what the budget is to obtain these needs. Originally initiated by Ascure's experience in Business Continuity Management, we use two steps to find an answer to following questions:

- What does management/Corporate Security Policy want to achieve
- What are the requirements for the IT department
- What does the business need

To answer these questions Ascure will

- Map the existing network by studying available designs and/or use 3rd party tools to map the existing network
- "Talk" by means of random interviews with all players involved to define the common goals/needs.
 - Management
 - IT Department
 - Business departments

Once all information is gathered we can chart the real business needs of your environment so that solutions can be found in an efficient and cost-effective manner.

Penetration testing

Ascure can not only help you with determining the strength of your logical security but also with your physical security. According to the client's needs a detailed overview can be given to assess your overall perimeter security.

Request for proposal

Once you know what you want, finding the best skilled partner or the best suited tools/appliances can be a difficult job. An adequate and complete RFP will save you time and a lot of money and is one of the key factors in a project's success. With a lot of experience in technical - and policy writing Ascure can help you create an adequate RFP by:

- Helping you to determine the proper procedure according to Belgian and European laws and regulations according to budget
- Helping you describe your exact need
- Guiding you in the use of the proper terminology

When the answers start rolling in Ascure assists Purchasing in determining the best-value-for-money analyzing all received responses and comparing them to predefined key points. Here is Ascure's experience and the fact that Ascure is vendor independent a key asset. This ensures you a solution tailored to your business needs, not our profit margin.

Architecture design and Quality control

Designing a network isn't an easy task to complete. Often there is a lack of available data concerning scaling, bandwidth and critical business systems. Ascure can help you with the design of your network security architecture as well as offer quality controls on designs delivered by your internal services or your preferred third party supplier.

Audits/analyses FW rules

FW rules are created when the need arises. However cleaning them up is often forgotten. Ascure can help you in maintaining your FW rule base up-to-date by

- Cleanup unused rules
- Evaluate the need for any "ANY" used and tighten where needed
- Advise you on potential security risks within certain rules
- Consolidate similar access rule into one rule

Log file analyses and correlations

Log files are usually very big and are an important source of information on what is going on on your network. Unfortunately most usage is restricted to troubleshooting. Ascure uses both in-house and 3rd party tools to analyze logs and make correlations. Ascure will provide:

- Analyze and report on most common rules
- Analyze and report on most common services
- Analyze and report anomalies in your log files such as port scans, ill configured services/devices
- Analyze what should be logged and what not
- Analyze potential external or internal breaches
- Provide feedback on the legal impact of what you log

Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.
(Sun Tzu)