



STORMSHIELD

OPINION ARTICLE

NETWORK & FIREWALL SECURITY: THE TOP 6 MISTAKES TO AVOID

Simon Dansette
Product Manager,
Stormshield

Buying a firewall is good. Deploying it correctly is better still. However, it's easy to make a mistake when configuring it, and this can jeopardise your entire security policy. We look at the most common errors when creating security policies, performing updates and ensuring consistent rules, and how to avoid them.

Firewalls are the cornerstone of IT security, and are of central importance when securing IT networks against cyber threats. But these tools need to be installed with care. We examine the six mistakes to be avoided when deploying firewalls.



FORGETTING TO PLAN


"In situations where an IT manager may have to manage a multitude of tasks, even the most seasoned IT manager can get distracted and make a mistake when setting up a firewall," says **Quentin Tieghem**, pre-sales engineer at Stormshield. So how do you address this issue? *"Plan, to make sure you don't miss anything, but also to make it easier to manage the firewall in the longer term."* In practical terms, mapping network traffic using a flow matrix provides a starting point for considering future firewall rules. *"Identifying network flows is a major task, but a necessary one. You then have to ask yourself how to position your firewall, which resources to protect or exclude, and what level of segmentation you need."* So, to make it easier to implement the firewall, you need to consider company-specific uses; for example to address the needs of teleworking employees, but also to identify which individuals might be required to administer the network. *"The basic principle,"* says **Guillaume Boisseau**, Professional Services Manager at Stormshield, *"is to first create a theoretical configuration, and then to verify that the rules work in practice."* Because the rules of a firewall are bound to change along with the network it protects, Tieghem advises that updating procedures should be planned in advance, even before the firewall is installed. *"Write a procedure from the beginning that explains not only how to set up the firewall, but also how to maintain it in an optimal working condition."*

USING THE DEFAULT SET-UP

"One of the most common mistakes is not fully configuring your firewall at the time of installation," Boisseau adds. The first step is to review the default services – or disable the ones you don't need – and choose new passwords that are as secure as possible. *"Particular attention must be paid to default administrator accounts,"* insists Tieghem, who recommends configuring them to restrict privileges to cover only the specific needs of each user. Another mistake is to leave a rule enabled, thinking that you'll come back to deal with it later... and then forget it. *"This is common, and hardly surprising in a profession in which the pace is often intense,"* Tieghem continues. *"There are two ways of dealing with this: you can force yourself to complete the process immediately, or create a time object with an end date for rules with a limited lifespan."* Also consider disabling the SNMP protocol or configuring it according to your needs: it enables network administrators to manage equipment.

OVERLOOKING NAMING

Boisseau says that another central issue is the naming of the networks and devices connected to the firewall. *"This is an issue that keeps coming up. My advice is always to stick to the existing rules. If you've already taken the trouble to name your servers with a DNS server, avoid problems by using that naming system."* It is also important to pay particular attention to changing business activities within the company. *"The typical example,"* he explains, *"is a server that has now being reused for a different purpose in a company, but is still identified on the network with the same IP address. So the server has changed, but the firewall rules haven't, and this server has rights that it shouldn't have"*






FORGETTING THAT THE WORST CAN HAPPEN

Even the most robust infrastructure can suffer a hardware or electrical failure. The challenge is to limit damage and maintain operational services as best as possible. *"Firewalls are often the main communication nodes in a company's IT network,"* says Tieghem. *"It is essential to integrate them into the disaster recovery plan (DRP) and business continuity plan (BCP), and to calibrate this integration."* The scale of the problem obviously differs depending on whether the firewall occupies a central place in the company's architecture, or whether a crash simply prevents a few employees from having access to emails. *"We need to test the implementation of DRPs and BCPs, and look beyond just the software component,"* says Boisseau, then adds: *"The reason that equipment has a high level of availability is to make sure that there is always a way to pick up any slack. So you have to make regular backups; but most importantly, you have to test the switchover between the main equipment and the backup."* Similarly, setting up a logging system from the beginning could save you a lot of trouble later on.

NEGLECTING TO MONITOR FILTERING RULES

A firewall is practically a living object, and not surprisingly, is bound to change as the company's business does: changes in the production process, increased use of teleworking, launching a new activity, etc. Security maintenance, again, is something that needs to be considered from the very outset of system implementation. *"Now that firewalls are increasingly at the heart of networks, any failure to keep rules up to date logically exposes the infrastructure not only to malware and ransomware, but also to any young geek who decides to launch an opportunistic attack using a rootkit,"* Tieghem points out. The engineer suggests a simple strategy for dealing with this risk: *"Record. Record everything."* *"You need to have a clear record of the rules and changes in the infrastructure over time,"* he says, *"to ensure you don't end up with lots of rules set up without any explanation, and thus an understanding of what they are there for."* The use of auditing tools will provide a precise understanding, enable checking of the use of rules and objects and highlight unnecessary procedures, but will not be sufficient to offer a detailed insight into how the infrastructure operates. *"It is perfectly possible to manually create a monitoring file with the added rules and keep a methodical history of changes to the firewall,"* says Boisseau. With this kind of archiving work, keeping your rules up to date and being aware of IP and URL filtering becomes much easier. *If the company uses a service provider, it is very important to ask for deliverables that provide traceability,"* he continues. *This type of record-keeping, whether internal or produced by an external company, also facilitates transmission by avoiding situations in which all the knowledge rests with the same employee."*



POORLY ORGANISED INFORMATION CHANNELS

Lastly, security maintenance also goes hand in hand with in-service maintenance. *“You need to update signatures as often as possible to avoid being vulnerable to new attacks, and remember to update the equipment itself, thus ensuring it’s always up to date with the latest maintenance patches and the most recent security elements,”* Tieghem explains. The experts confirm it: anticipation is the key to avoiding errors and reducing workload in the long term. *“At the implementation stage, consider subscribing to RSS feeds and other informative tools for the solutions you use,”* Boisseau says. *“This is the best way to get early warnings of vulnerabilities identified in the software components that make up the firewall, and quickly install patches for any bugs and security flaws that arise.”*

In-service maintenance is also accompanied by regular maintenance on the infrastructure – a key issue that deserves (another) article in itself.



STORMSHIELD



Stormshield, a wholly-owned subsidiary of Airbus CyberSecurity, offers innovative, end-to-end security solutions for the protection of IT networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

www.stormshield.com