Mail Protection
- SANDBOX -

THE CUSTOMER

The customer is the largest bank operating in a central African country, a market leader. This financial institution offers both retail and depository banking services. Its customer base is made up of major private-sector accounts, institutions, SME's and private individuals. The bank is present across the country, including the more remote and isolated regions.
For more than ten years, SONEMA has worked hand in hand with the customer supplying VSAT connections for its main branches, in addition to supplying value-added services including hosting for virtual servers, videoconferencing, IP telephony, bandwidth optimisation and managed services for firewalls.

THE CHALLENGE

The customer's staff complained to the IT Director about lengthy delays to receive emails. The IT Director was therefore regularly asking SONEMA to manually add new firewall rules blocking email addresses which were seen as a major source of spam. As this type of filtering is ineffective, SONEMA carried out an audit to check both the company's Internet connection and incoming email traffic in order to identify the source of the spam emails.

The audit carried out by SONEMA's technical team showed a problem of recurring spam (roughly 80% of the email traffic was spam). The content filtering carried out by the Internet firewall was inadequate as most of the spam messages were encrypted between the spam servers and the customer's mail server and the spam mail was able to get past the firewall which was causing congestion on the Internet connection.

SONEMA'S SOLUTION

SONEMA advised the customer to install the "*Mail Protection*" solution which filters incoming emails. This solution enables SONEMA to scan both encrypted and non-encrypted emails and to block viruses, malware and known spam operations in addition to zero-day attacks with no known signature thanks to the optional "*Sandbox*" feature.
Through this offer, SONEMA was able to put in place appropriate solutions in order to protect the customer's email system by redirecting the incoming email traffic to SONEMA's premises in Frejus, France where it is filtered and analysed before being delivered to the company's email server.

Furthermore, the "*Mail Protection*" solution suited the customer perfectly as he didn't wish to invest in a costly solution and did not have security experts available to install and manage this type of service. By subscribing to this service for the cost of a monthly subscription based on the number of mail boxes he wanted to protect, the customer has delegated the installation and management of the solution to SONEMA.

For the service implementation, **a proxy mail server was installed between SONEMA's network and the bank's** mail server in order to analyse incoming emails before they reach the bank's mail server and are delivered to the end user.

The filtering is carried out in 3 steps :

- **Step 1 :** Email traffic is redirected towards the relay mail server. This server offers a first level of protection by scanning emails with antivirus engines, IPS, IP reputation analysis and URL filtering. As the relay server is the connection's termination point, it is able to decrypt message content in order to apply these protective measures.

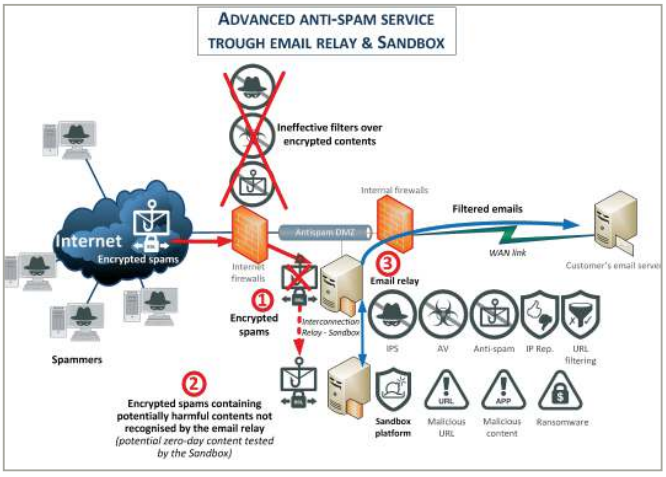

Figure 1 - Example of Sandbox filtering

- **Step 2 :** If the message contains an attachment or a URL, it is transferred to the *Sandbox* via a secure channel. Once in the *Sandbox*, the message is executed in a virtual environment which resembles a work station. As the attachment or URL is executed in the test environment, its behaviour is automatically recorded and analysed by the *Sandbox* module.

  In the event of any suspicious behaviour (files deleted, system settings changed, remote connections, etc...), the *Sandbox* module blocks the message directly and either deletes it or puts it in quarantine.

  This second step enables filtering for emails containing zero-day malware codes. These codes are created by hackers as a targeted attack on the customer, designed to exploit software flaws as yet unknown to editors of antivirus-programs.

- **Step 3 :** After filtering, legitimate emails are sent to the customer's email server by the relay server.

In order to improve email security, this procedure allowed SONEMA to **eliminate roughly 80% of unwanted network traffic on the customer's Internet access**.

CONCLUSION

The whole experience was very positive for the customer, as the solution allowed him to enjoy the following advantages :

1. Advanced email protection with the very latest email filtering technologies;
2. Reduced operational costs, the customer did not need any technical staff to carry out this solution or invest in a specialised platform;
3. Benefit from a scalable platform (licences, software, hardware) ;
4. Reduced installation time (about 15 days) in comparison with an equipment-based solution (which needs to be ordered, installed and set up) ;
5. Simplified invoicing based on the number of mail boxes and the number of incoming mails ;
6. Reduced congestion on the Internet connection and customer's mail server by filtering incoming email traffic ;
7. Performance improvements (disk space, processor, random access memory) of the mail server by reducing the incoming traffic.

For further information:
sales@sonema.com