signal
**IT**solutions

PROXY

## Proxy… (Secure Web Gateways)

So, you are a network admin, in charge of a small to medium size IT environment. Endpoint management is key to keeping the network functioning as it should, Anti-Virus is installed, Anti-Malware is installed and you have a healthy patch management utility that keeps all machine OS's (including Servers) up-to date.

You may be using on prem exchange, Office 365 or Gmail for business. Your **information security policy** (ISP) is up to date and staff have all signed it to confirm they will comply with how the IT network is to be utilised. You carry out random phishing **experiments** on a quarterly basis to understand if staff have headed the warnings about trusting email and web content that they may receive or utilise on a daily basis. **These phishing experiments tie in nicely to the education you provide twice yearly to all staff based on the latest internet threats that exist or that they could be subjected to.**

And finally, the Social Engineering role plays conducted with front of house staff, and Finance make for an altogether safe IT environment. To compliment the social engineering training provided you also cover **Vishing and Smishing** for staff members who are issued with a company mobile phone.

## Scope…

The reality of the situation is you might be undertaking some of these best practice elements, but not all. Irrespective of what you are undertaking currently, the fact of the matter is you are in part reliant on your staff member making the "right call" when presented with a situation or circumstance.
You might have staff that travel. They may utilise free WIFI or "open" networks to create a VPN tunnel back to the corporate network for access to systems and or documents that are on the network.
The corporate device they are using to connect might be an image that allows browsing the internet off of the domain, how can you further safeguard the endpoint in circumstances such as this and when that device is on the corporate domain either remotely via VPN or locally within the network.

## The resolution…

It's difficult to mitigate all potential risks on a network at any given time, however extra levels of protection do exist, whether the user is connected on the network or not.

Secure Web Gateways come in many different guises, agent and browser driven, but are now becoming essential in the protection of endpoints and ultimately the network estate. Phishing activities are becoming more of a threat and ever sophisticated in relation to their look and feel and the way they are executed.

More worryingly is the **"personalisation"** of these activities which adds significant authenticity to the request.

Outside of just Phishing attempts is the security wraparound in relation to how SWG's can examine the potential payloads within email such as **embedded links, the ability to identify profanity within emails, and the ability to recognise certain images** that otherwise your users should not be subject to.

Add this type of email protection combined with web protection to guard against users accessing web content that they should not – non validated URL's, potential URL's with payloads, sexual and violent web content, then a SWG starts to become an attractive additional protection method against aspects that are not in a network admins control, that being human error and or human misjudgement.

Many SWG's use open DNS capabilities which mean you don't need to be connected (via VPN) to the main corporate network to safeguard an endpoint device for users that travel.

Signal Networks recently implemented an SWG to complement our clients existing endpoint security.

The Client, a global pharmaceutical noticed an increase in SPAM emails inbound via their O365 deployment. In addition, the Client did not have a focused staff training regime that the IT department undertook on a regular basis to inform users of potential threats.

Working with our client we introduced the benefits of SWG's as additional piece of mind and configured email and web capabilities to provide that extra level of protection to compliment protection that was already in place.
During the initial proof of concept (POC), the recording of email and web activities

was undertaken to provide a working policy that was to be adopted across the organisation. That initial logging provided an interesting but worrying pattern of the types of email and web request that were being sent and received in to the organisation, and the type of web requests being made to the Internet from the network.

A policy was adopted and implemented which locked down the environment based on the initial discovery of the types of activities being recorded.

Key to the adoption of this policy was to keep in mind the usability of the solution, the whole purpose of the SWG's introduction was to safeguard but at the same time not to inhibit staff and productivity.

Outside of the policy enablement was the audit capability this now provides to the client based on staff activity and efficiency.

This is now more important than ever based on compliance levels that many organisations now adhere to in relation to delivery of IT services.

## Related considerations…

- Is O365 enough to safeguard my email environment – do I need an SWG?
- I am looking at areas of compliance within my IT network and across the organisation as a whole, does Cyber Essentials dictate that I need an SWG?
- I have no real logging activity or capability on my network currently around staff browsing habits, will an SWG provide me with granular logging?
- Can proxy or SWG protection transcend my mobile estate?
- How do SWG' s tie into Information Security Policies (ISP's).

SWG's provide additional capabilities that compliment protection you may already be utilising.

We can guide you through the pros and cons of different solutions and configure a policy that operates to provide additional piece of mind and protection within the network.

Internet based SWG's provide that critical layer of protection at the INTERNET LEVEL. Filtering at this level means potential payloads via email or compromised websites don't make it to the ingress point of your network.

## Let's talk.

We understand every business is different and that's why we offer a complimentary consultation to discuss your needs…

0333 370 2202