To proxy or not to proxy

By Andrew Wilson

23 Nov 2017

Traditional methods of effectively securing connections on a corporate network usually revolve around proxy solutions. In an enterprise network environment, a proxy server acts as an extra layer of security between business servers and outside traffic, preventing cyber breaches and controlling incoming and outgoing connections. While proxy solutions are complicated to implement and require configuration and management of each device connecting to the network, the security level afforded by proxy connectivity is invaluable in the fight against unauthorised access into organisations networks.

These days, however, everyone wants to take their smartphone, tablet or notebook computer to the office and connect to corporate servers and applications with ease. In addition, given that proxy servers are not known for being hassle-free, and the fact that most mobile devices and their applications are not exactly proxy-friendly, organisations are feeling the pressure to allow employees to make direct internet connections, that is, not via the proxy, from these devices. Generally, this would mean punching a hole directly through the firewall to enable the connection and here, security is sacrificed for productivity. Ironically, this is a sacrifice that some organisations aren't even aware they're making, let alone how risky it is.

In such cases, where the business faces internal pressure to allow direct access connections, the organisation forgets about the external risk of hackers looking for somewhere lucrative to initiate a ransomware attack. Therefore, it begs the question, in the age of mobility, should organisations have to choose between productivity and security? The answer is no. As to whether an organisation should proxy or not, the answer to that merely requires more time.

The future is not to proxy, but what about security?

By looking at the pace and trends of technological developments, it is apparent that the future for proxy solutions is going to become more challenging. The pressure to allow users to 'bring your own device' will increase and the device will undoubtedly be configured to access the internet directly. In addition, configuring this device to use a proxy is a hassle at best, and at worst, not possible.

Since the proxy server has also become the primary point at which to control corporate network security and disable

certain connections and actions, the question is how does one allow direct internet access and not compromise the organisation's policies?

Does not play well with others

As already established, the introduction of smartphones, tablets and other internet of things (IoT) devices means the future of proxy becomes challenging because all of these Android and Apple devices are not proxy-friendly. Although browsers are typically easy to configure to work with a proxy system, many applications will not work without direct internet access.

My advice has always been that it is preferable to have employees in a proxy environment for a large business network as opposed to allowing direct internet connectivity as it gives the corporate more control. These direct connections that employees and devices are insisting on are becoming unavoidable. As direct access becomes more widespread, it comes at a security cost: less visibility of and less control over the connections within the network.

In other words, each and every mobile phone, laptop, tablet or smart printer that is 'allowed' to have unmanaged direct access to the internet is a vulnerability. It's potentially a risk that no one is thinking about, or even aware of. It also highlights the need for technological solutions to control these direct connections to ensure that security accompanies mobile productivity, as choosing between them will become less practical and increasingly risky.

The future is already here

Today, the majority of cyber security measures are still proxy-based as these offer the most control, and this is not going to change. Proxy measures will always offer the highest levels of control. However, for those organisations where the pressure to allow direct connections has become overwhelming, this will create a requirement for solutions that go beyond firewalling and offer more flexibility than proxy.

Such organisations aren't going to be looking to proxy to solve their security problems. Instead, they should look for security solutions and products that provide safe, managed direct access to the internet, without the traditional challenges posed by proxy. They should look towards solutions that deliver visibility into network traffic and user activity.

You can't manage what you can't see, and we firmly believe that the first step in security is visibility. It is for this reason that companies should look for solutions that offer the benefits of proxy-type control over direct access connections with the ability to spot ransomware, pinpoint vulnerabilities and identify any other potentially dangerous 'phone-home' connections.

ABOUT THE AUTHOR

Andrew Wilson is CEO at LucidView.