Firewall Configuration Impacts

Business firewalls are essential for security, as they block unauthorised communication between the business network and the outside world. This prevents direct access to user devices and can restrict access to servers, which have specific requirements for connection. Firewalls have various uses beyond blocking this external communication (Stewart, n.d.), and as such are a solution to many different problems. A few examples of these uses are:

- Blocking access to unauthorised webpages
- Measuring the amount of traffic through the firewall
- Blocking malicious code and communications
- Blocking unauthorised access to any device on the network from outside the network

The consequences of not having a firewall or not having a firewall set up are considerable. Having unauthorised communication take place allows for malware to spread through the network, as firewalls are key to preventing some types of malware. Additionally, any of the benefits described above are lost (Ranbe, n.d.).

Having the firewall set up wrong allows for some issues, as it may not properly block unauthorised communications or malicious code. This isn't as large of an issue as not having a firewall entirely, however patching the holes in the firewall is an important solution as the risk of leaving them unpatched increases over time, as there's more opportunity for the loopholes to be abused.

Should a firewall have rules that are too aggressive, however, it may inhibit proper use of the network, preventing access to certain webpages like search engines and research sources, which may inhibit productivity. Similarly, a rule that restricts access to a server may make work impossible should it rely on data stored on the server. An example of this could be a file hosting server that has a rule that excludes the port that the FTP protocol uses.

VPN Configuration Impacts

VPNs are used by businesses to allow remote users to connect to the private network in a secure way. This allows for the transfer of private company data in a safe way, allowing people to work from any location without having the data be intercepted. This concept is useful for businesses of any size, allowing for people working from home or on business trips, anything that takes place outside of the office (Verizon, 2018).

There are some obvious issues that can take place with VPN configuration issues. VPNs route traffic through an external server and onto the company network, and issues with that routing could result in a lack of communication for the client, preventing any work from taking place should it require this communication.

As well as this, VPNs rely on encryption to keep the data safe, and, while it's unlikely, unencrypted VPN traffic could jeopardise the usage of a business VPN. Having the data that's communicated over the VPN be accessible, whether it's because the encryption isn't applied or because the encryption standard used is unsafe, defeats the purpose of using a VPN in the first place (Posey, 2019).

Setting up a VPN can be complicated as there's a lot of different protocols for communication. There are five primary protocols used for VPN connections in the modern day, specifically PPTP, SSTP, L2TP, OpenVPN and IKEv2 (vpnMentor, n.d.). Each of these protocols have benefits and drawbacks, a few of which have key issues that mean they shouldn't be used at all.

PPTP is a protocol and encryption standard made in 1999 (vpnMentor, n.d.) that is known to be insecure, with many reports stating that the protocol can be cracked quickly, and that the NSA in particular has a method for decrypting data transmitted using PPTP (vpnMentor, n.d.) (Gordon, 2017). This means that this protocol shouldn't be used for any important information and possibly shouldn't be used at all as there are alternatives that are just as simple to use that aren't compromised.

As well as the issues PPTP has, a few of the other protocols have issues with firewalls. L2TP and PPTP are both easily blocked by firewalls as they both use specific ports for communication, which can be blocked easily. SSTP, for example, can circumvent firewall blocks by using other ports, namely port 443 (vpnMentor, n.d.) which is used for TCP, specifically used for HTTPS (orosk.com, n.d.), which is considered essential. This links back to the firewall configuration impacts, as blocking port 443 to prevent VPN connections also blocks HTTPS connections.

Finally, third-party VPNs rely on a third-party hosting the VPN that facilitates communication between the users and the network, having all the information pass through their servers, and having them own the servers and configuration of the VPNs that are in use. This means

that the third-party has more control over the way that the data is handled than the company itself, which is a potential point of failure.

Bibliography

Gordon, D., 2017. *PPTP VPN Concerns*. [Online]
Available at: https://www.myworkdrive.com/vpn-alternative/pptp-security-risks/
[Accessed 15th November 2019].

orosk.com, n.d.. *What is Port 443? Use of Port 443.* [Online]
Available at: https://www.orosk.com/what-is-port-443-use-of-port-443/
[Accessed 15th November 2019].

Posey, B., 2019. *How to fix the four biggest problems with VPN connections.* [Online]
Available at: https://www.techrepublic.com/article/fix-the-four-biggest-problems-with-vpn-connections/
[Accessed 15th November 2019].

Ranbe, R., n.d.. *What Happens if a Firewall Is Disabled?*. [Online]
Available at: https://smallbusiness.chron.com/happens-firewall-disabled-62134.html
[Accessed 14th November 2019].

Stewart, G., n.d.. *The Top 5 Reasons Why Your Business Needs a Strong Firewall.* [Online]
Available at: https://www.suretyit.com.au/blog/the-top-5-reasons-why-your-business-needs-a-strong-firewall/
[Accessed 14th November 2019].

Verizon, 2018. *What you need to know about business VPN.* [Online]
Available at: https://go.verizon.com/resources/what-you-need-to-know-about-business-vpn/
[Accessed 15th November 2019].

vpnMentor, n.d.. *VPN Protocol Comparison: PPTP vs SSTP vs OpenVPN vs L2TP vs IKEv2.* [Online]
Available at: https://www.vpnmentor.com/blog/vpn-protocol-comparison-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/
[Accessed 15th November 2019].