POINT OF VIEW

Why Security Is a Top Influencer of Network Performance

Introduction

To stay competitive, a high-performing network that meets the needs of digital acceleration initiatives is critical. Sometimes it's difficult to know what to focus on, as there are a lot of different factors that can impact performance—from the architecture chosen, to the age of the equipment, to the client devices. Another key contributor that is often overlooked is network security (or lack thereof). In this paper we'll explain some of the ways that network performance is impacted by whether or not certain security controls are in place.

95% of traffic is encrypted across Google as of December 11, 2021. [1]

How Security Impacts the Network

Load on the network often comes down to who is on the network and what they're doing. Security has a lot to say about both of those factors. Effective security gives control over who is on the network at any given time and what they have the ability to do. This encompasses which applications they run and what resources they can access.

For local-area networking (LAN) purposes specifically, traffic must be inspected in order to perform accurate application control, which affects the load on the network. In terms of overall security, many organizations have had to choose between security and performance, as subpar firewalls could not keep up with the traffic, causing bottlenecks. Turning off security in favor of performance is not a viable option given the huge volume of threats that hide in HTTPS traffic.

LAN-level Security Features That Contribute to Better Performance

Access Control

Access control is all about who gets on the network and what they have access to. Without it, devices that shouldn't be on the network can attach and potentially burden network resources unnecessarily. Having consistent policies controlling who can access the network and what they can do improves overall network performance by limiting needless traffic and preventing overuse of key resources by clients that don't have a business need to use them.

Authentication

A subset of access control is authentication, which ensures that a user really is who they say they are. The more reliably a user can be validated, the more certain IT can be that only people who need networking resources are accessing them. Zero-trust network access (ZTNA) architectures validate rights and security posture at all stages of access. As network and application performance are often highly impacted by how many devices/users are accessing them at the same time, fine-tuning control over how many devices and what users are online can directly improve network performance and user experience.

Guest Networks

Many business initiatives require the need for non-employees to have some level of network access. Guests on the network are already a potential security risk, but if not properly controlled, guests can also be a performance risk. Having no application or bandwidth controls on guest users can result in network resources being dominated by noncritical devices running personal applications. Having a strong security policy with controls on what guests can and can't do improves network speed for everyone.

IoT Devices

Internet-of-Things devices are important for digital acceleration, enabling key business initiatives that would be slower to implement without them. But these devices are known to be security threats, as they typically have little to no built-in security, and can be easily compromised. Knowing what IoT devices are in the environment and implementing correct security policies for them can help to ensure that misbehaving devices or "runaway" applications do not bog down the network unnecessarily.

IOC Containment

One very beneficial tool for securing IoT devices is the ability to contain devices that are being compromised, automatically. Malware on a compromised device is not only a security risk to company data, but malware processes are often network-intensive (as they comb the network looking for valuable data) and can slow down performance for the wider user base.

Traffic Inspection

Traffic inspection is a double-edged sword. With the amount of encrypted traffic in use, having traffic inspection is the only reliable way to offer the application control necessary to offer improved performance to business-critical devices. This also allows for limiting personal traffic to lower network impact. Further, if viruses, malware, or other threats get into the network by hiding in encrypted traffic, the result could bring the network to a standstill. However, depending on the equipment chosen, traffic inspection can have unintended consequences on network performance.

Conclusion

While certainly not the only factor, security plays an important role in network performance. It should be carefully considered and implemented with an eye on optimizing user experience in every possible area. A well-secured LAN is much more likely to be a high-performing LAN.

[1] "HTTPS encryption on the web," Google Transparency Report, accessed December 28, 2021.

FORTINET

www.fortinet.com

January 12, 2022 12:17 AM
1181055-0-0-EN