Scaling the Library Resources with Zscaler

Anu Moorthy and Barbara Dietsch

Abstract

More and more institutions and universities are implementing security measures to prevent wide-spread cyberattacks. When institutions initiate new security applications, the library is often overlooked. Libraries have complex ecosystems where multiple applications and systems converge with user data and online library resources. These ecosystems have various considerations including multi-factor authentication, proxies, multiple virtual private networks (VPNs), knowledgebases, and vendor inconsistencies. Duke University Health recently launched data security software called Zscaler, which prevented on-campus users from accessing the library e-resources. This presentation describes how Duke University Medical Center Library staff discovered the access issue and tested various workarounds to allow patrons to access library e-resources. The discussion covered how staff continue to work with Duke University Health IT security staff and university administration to find resolutions for the complex integration of security software with the library's online resources.

Keywords: electronic resource troubleshooting, remote access, identity and access management, cybersecurity, network security, zero trust, zero trust architecture

Duke University Medical Center Library (DUMCL) provides the services and collections necessary to further educational, research, clinical, and administrative activities in the medical field. The library primarily serves the Duke University Medicine faculty, staff, and students in the Duke University School of Medicine, Duke University School of Nursing, allied health programs, and graduate programs. The library also serves Duke University Hospital and Duke University Health System.

The library collaborates closely with Duke University Libraries (DUL) in providing access to many online journals, e-books, and databases. However, DUMCL handles all acquisitions, renewals, and maintenance of their unique subscriptions and purchases.

In September 2021, staff at both DUMCL and DUL began to receive a large number of online access issue tickets. Most of these tickets were from users on campus, and lack of access was for all library e-resources including e-journals, e-books, and databases. After extensive investigation, Moorthy and Dietsch determined that the users with access issues were working while on the Duke Health campus and/or were using a Duke Health-issued computer or laptop (See Figure 1). It was perplexing since library staff at both DUMCL and DUL could access the library resources from on-campus and off-campus via VPN or through proxy.

"VPNs, or virtual private networks, are services that create a secure, encrypted connection from one computer to another. Similar to a proxy, a VPN acts as a middleman for a computer and its destination, sitting between them and overriding the connecting computer's IP address with its own. However, unlike a proxy, a VPN is more secure because it encrypts a computer's information before it even connects to the internet."[1] A VPN allows users to access the Internet as though they are connected to a private network such as the Duke University network. When using the VPN, library users access the library's e-resources as if they are on-campus and therefore do not have to use the proxy. "Proxies are a type of intermediary server or software system that sits between one computer and another. Libraries commonly employ proxies to authenticate remotely located patrons because a proxy enables a library to override a patron computer's IP address with

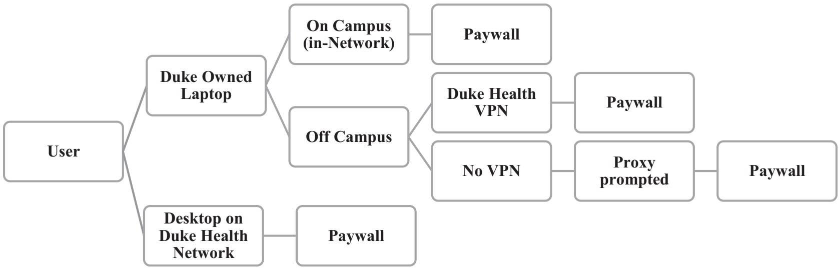

Figure 1.

its own, thus changing the computer's apparent location. The most commonly employed proxy system for libraries is EZproxy."[2]

We were initially unable to resolve these Duke Health access issues using the normal troubleshooting channels. Since we could access the library e-resources and were on campus, we began to suspect it had something to do with Duke Health computers or systems. We requested a screenshot of the user's Internet Protocol (IP) location utilizing the ShowMyIP.com website (see Figure 2). The first irregularities we noticed were that the location was not Durham, North Carolina, and the IP address was not within the library IP ranges. We also noted the Internet Service Provider (ISP) was Zscaler, Inc. After an Internet search for information about Zscaler, we learned it is a third-party Cloud security application. We went back through our troubleshooting tickets and realized that the majority of the tickets were for Duke Health patrons. We deduced that these users had Zscaler installed on their Duke Health-issued computers, which was interfering with on-campus access to library e-resources.

At this point, we contacted Duke Health System's Information Technology (IT) department. Because of the millions of daily security breach attempts, IT staff had installed Zscaler on many of the Duke Health-issued computers and laptops. The goal of Duke Health IT is to eventually have this Cloud security application installed on all Duke Health computers and laptops to protect the integrity of Duke Health systems, networks, and devices.

Details:

Your IPv4	**136.226.53.17**
Your IPv6	Not found!
Country	United States
Region	Maine
City	Bangor
ZIP	04402
Timezone	America/New_York
Internet Service Provider (ISP)	ZSCALER, INC.
Organization	Zscaler, Inc
AS number and name	AS22616 ZSCALER, INC.
User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36

Figure 2.

Zscaler and Zero Trust Architecture

According to National Institute of Standards and Technology (NIST), "A typical enterprise's infrastructure has grown increasingly complex. This complex enterprise has led to the development of a new model for cybersecurity known as "zero trust" (ZT). In this new paradigm, an enterprise must assume no implicit trust and continually analyze and evaluate the risks to its assets and business functions and then enact protections to mitigate these risks. A zero trust architecture (ZTA) is an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement."[3] The cybersecurity Cloud application, Zscaler, utilizes this zero trust security model (see Figure 3).

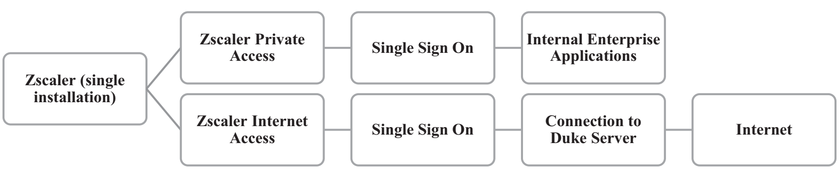

Figure 3.

How Zscaler Affects Access to Library E-resources

When a Duke Health user is trying to access Duke authorized applications or software that require Duke authentication, Zscaler allows the user to access the application. However, if the user tries to access any unauthorized Cloud applications or Internet resources, Zscaler rejects the user from accessing the resources from the Duke device. If the user tries to access a licensed library resource from a computer that has Zscaler installed on it, the publisher or vendor sees the cybersecurity application's masked IP address location and rejects the user from accessing the resource (see Figure 4).

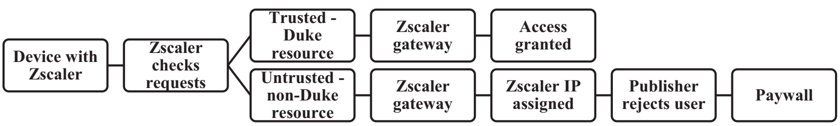

Figure 4.

Duke Health IT was not aware that Zscaler would interfere with access to the library's licensed resources. Once library staff described the complex setup of the library's resources to Duke Health IT; a team was formed to brainstorm and outline the processes to restore access for users. The team met several times a week for more than six months.

After the first potential work around of redirecting users to proxy authentication, the number of tickets was greatly reduced (see Figure 5). However, we were still getting complaints from users about other access problems. We formulated solutions for each unique access issue that was caused by Zscaler. This took much creativity and thinking outside of regular troubleshooting strategies. Resolution and user communication took considerable amount of staff time.

One of the next steps was for the librarian to identify and curate the library's licensed electronic resources to find the root uniform resource locator (URL) for all publishers and vendors. Duke Health IT then uploaded over a thousand URLs to Zscaler. This created an exceptions list that allowed affected users to access the library's licensed resources.

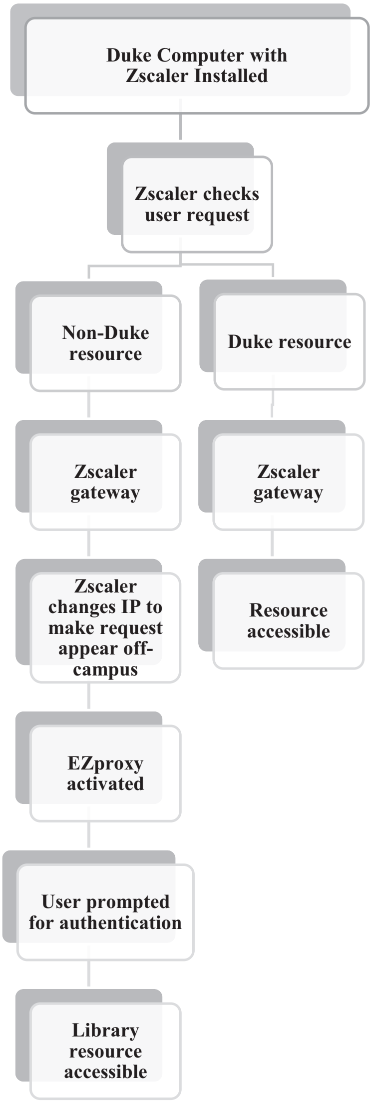

Figure 5.

Zscaler used the exceptions list to check and confirm that these were trusted resources. For the most part, this solution worked. However, every time a publisher or vendor made any changes to a URL, the access issues returned. When users reported access issues, we consulted the exceptions list and updated the root URL. Due to the workload and the extent of the changes, Duke Health IT installed two additional servers and hired two additional staff members.

The complex infrastructure of library, IT, and authentication systems can serve as an obstacle to seamless user experiences. At DUMCL and Duke Health, cybersecurity software rollout helped library staff to learn about cybersecurity protocols and standards. Because of this, we were able to approach troubleshooting in more creative ways and use new techniques. This also allowed us to educate users and IT staff about the complex ecosystems of the library.

Acknowledgments

Anu Moorthy and Barbara Dietsch express their sincere thanks and gratitude to Steve Oates and Michael Ravenel-Baker for their expertise and assistance.

Contributor Notes

Anu Moorthy is Electronic Resources Librarian, Georgia Institute of Technology, Atlanta, GA, US. She formerly was with the Duke University Medical Center Library.

Barbara Dietsch is Electronic Resources Management Specialist, Duke University, Durham, NC, US. She formerly was with the Duke University Medical Center Library.

Notes

1 Holly Talbott and Ashley Zmau, *The Electronic Resources Troubleshooting Guide* (Chicago, IL: ALA Editions, 2020).
2 Talbott and Zmau, *The Electronic Resources Troubleshooting Guide*.
3 Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly, "Zero Trust Architecture," *NIST Special Publication 800–207*, (August 2020), accessed August 4, 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.