Balancing risk with virtual private networking during a pandemic

Andrew Korty*
Chief Information Security Officer
Indiana University
535 W. Michigan Street
Indianapolis, IN 46202
U.S.A.
ajk@iu.edu

Daniel Calarco
Associate Vice President for Client Services & Support
Indiana University
2709 E. Tenth Street
Bloomington, IN 47408
dcalarco@iu.edu

Mark Spencer
Manager of Campus Network Engineering
Indiana University
2709 E. Tenth Street
Bloomington, IN 47408
maespenc@iu.edu

*Corresponding author

This is the author's manuscript of the article published in final edited form as:

Korty, A., Calarco, D., & Spencer, M. (2021). Balancing risk with virtual private networking during a pandemic. Business Horizons, 64(6), 757-761. https://doi.org/10.1016/j.bushor.2021.07.011

Balancing risk with virtual private networking during a pandemic

Abstract

When the pandemic struck and teaching went online worldwide, universities had to make pressing decisions that balanced cybersecurity against other factors, including health and safety, usability, and cost. One such challenge Indiana University (IU) faced was how to accommodate the secure telecommunications needs of 130,000 faculty, staff, and students who would now be teaching, learning, doing research, and working from home. Some universities reflexively promoted virtual private network (VPN) use for all activities. Such an approach would have been unsustainable at IU, however, owing both to the licenses and resources needed for the sheer number of users and to the high-throughput applications on which they rely. Perhaps even worse, it would have increased the chances that the VPN would be unavailable during a critical incident or other situation in which secure communications must be guaranteed. Instead, IU launched an awareness campaign demonstrating exactly when VPN use is and isn't needed. In addition, network staff employed a VPN feature called split tunneling to reduce the load. This article discusses the advantages and disadvantages of this approach and how IU made the decision to balance both sides of the risk equation to ensure the continued advancement of its mission throughout the pandemic.

KEYWORDS: Virtual Private Network; VPN; Information technology; Remote learning; COVID-19

1. IT at Indiana University

Indiana University (IU) is a large public research university in the United States. The university—with seven campuses, nine centers for medical education, and two academic centers across the state—does not have a "system" office like the University of California or University of Illinois. Rather, much of the administration—including IT, research, facilities, finance, marketing, and communications—is handled at what is called the "university" level, and applies across all campuses and centers. There are smaller campus-level administrative offices, with Bloomington and Indianapolis having more sizable operations than the other five campuses. Each year, IU educates over 100,000 students and employs over 20,000 faculty and staff across the state and online.

Information technology (IT) at IU is largely administered at the university level. The Office of the Vice President for IT and CIO (OVPIT) is a university-level office that provides IT to all campuses, has an annual budget of about $200 million, and employs approximately 1,100 full-time staff and 300 part-time staff. Functions in OVPIT include enterprise systems, networks, client services and support, learning technologies, research technologies, information security, and constituent relationship management (CRM). IU has a single enterprise resource-planning system for all its campuses and centers. The campuses' wired and wireless networks are all centrally administered with common hardware, configurations, policies, and ticketing. Similarly, IU's virtual private network (VPN), used by faculty and staff across the state, has appliances located in its Bloomington and Indianapolis data centers that are configured as one service to provide redundancy to all campuses.

2. IT's role in taking all teaching online at IU

The IT organization at IU has long been committed to business continuity and disaster recovery planning. Units are required to submit and update plans annually. There is a standing incident-management team executive policy group, which meets monthly and is organized according to Federal Emergency Management Agency (FEMA) structure. Each section—logistics, planning, operations, public information, etc.—has regular meetings, obtains required FEMA training certifications, and participates in an annual emergency management exercise.

In 2010, IT staff developed keepteaching.iu.edu in response to the H1N1 influenza pandemic. The site aggregated resources on how to move from in-person to online instruction if needed and walked faculty through the steps and best practices for remote education. The site was repurposed by many universities across the country during disasters such as the California wildfires in 2019 and the COVID-19 pandemic.

In addition, in 2018, the IT organization at IU conducted a daylong tabletop exercise on moving to remote work and instruction caused by a pandemic flu. Over 200 staff were immediately sent home or to work in an individual office away from their team members and had to figure out on the fly how to coordinate with their coworkers over Zoom. The lessons learned and after-action report provided a blueprint for the university of what to do during the COVID-19 pandemic.

3. What are VPNs and split tunneling, and how do they relate to pandemic?

In higher education, we're no strangers to remote work. We have been facilitating it for decades to allow for distance education, collaborative research, and staff flexibility in how they do their jobs. Remote work does, however, raise some IT security issues.

The first issue is access. It is common for maintainers of certain IT servers to limit access, especially when sensitive data is involved, so that only on-campus computers can connect. This approach locks out most would-be attackers, like building a big wall around a village. Unfortunately, it locks out remote workers too.

The second issue is communications privacy. A remote worker's connection to a university server has to stretch a long way, transiting their home network, the networks of various internet providers, and so on. There are many points along the line where an adversary could eavesdrop and collect information about the connection and the sensitive servers involved, or even access the data being exchanged.

VPNs are a common solution to both of these problems. When you use a VPN, you first authenticate with your username, password, and perhaps a second factor, like a code that is texted to you; then, the VPN software creates an encrypted *tunnel* over which all your internet traffic flows. One end of the tunnel is at your computer; the other end is on a VPN server in your organization's data center. Thanks to the encryption, once traffic flows into the tunnel, it cannot be examined or altered until it emerges from the other end. That traffic then appears as though it is coming from the VPN server, not your computer. So, if a server in your organization only allows traffic from inside the organization, you will be allowed to connect to it from your computer at home using the VPN. No unauthorized users are able to access that system because they would not be able to pass the authentication step. And no one between your home and the organization's data center can see the communications between your computer and the server, or even that those communications are happening at all.

Note that the security provided by VPN is only as good as the security of the VPN service itself. The VPN product must be from a reputable vendor with sound software development and vulnerability disclosure (e.g., "bug bounty") processes. Just as important, IT staff responsible for the VPN service must follow sound maintenance practices, from protecting administrative access to change management to patching. An attacker who is able to gain unauthorized access to the VPN server could undermine all of these protections.

This approach works well enough to solve the two issues mentioned here, access and communications privacy. But a lot of the traffic you generate is *not* destined for your organization's data centers. Most organizations are now using cloud services in some capacity, so much of the email, file sharing, and even videoconferencing activities are being processed in a far-away data center owned by Amazon, Microsoft, Google, or some other provider. Does it make sense to send that traffic over a VPN tunnel to your organization, only for it then to go out the organization's internet connection to one of these external parties? No. It would be much more efficient for that traffic to be handled by your home internet provider, saving the organization bandwidth, VPN license fees, internet usage fees, and so on. This approach is called *split tunneling* and is a feature of the VPN. With split tunneling enabled, the VPN sends only the traffic destined for your organization's networks through the VPN tunnel but allows your

internet provider to handle all other traffic the way it normally would. This approach can also provide a better user experience in using services outside of the organization.
VPNs' encryption of traffic can add overhead and affect the performance of a service, especially where communications applications such as Zoom and Teams are involved.

Some would argue that split tunneling introduces unacceptable risks. Usually, this argument is based on the notion that split tunneling might allow an attacker to break in to a user's computer from the internet and then use the VPN connection to access the organization's systems. This argument does not carry much weight, at least in a university environment, for two reasons. First, supposing split tunneling were disabled, the user's computer could just as easily be infected with malware when *not* connected to VPN, and then university systems would be exposed to that malware once the VPN is engaged. In fact, in today's threat landscape, that scenario is *more* likely. Second, if VPN resources are limited, *not* using split tunneling would mean limiting the scenarios in which the VPN can be used at all, reducing security in those scenarios. For these reasons, we believe use of split tunneling offers a net gain for security. Still, it is important for each organization to conduct its own analysis and to determine the right approach for its situation.

4. Pandemic strikes

In the lead-up to the coronavirus pandemic in the United States, IU began in February 2020 having weekly, then triweekly, and then daily emergency operation center briefings, with IT contributing to the planning. Areas of concern that were identified before the national shutdown included:

- *VPN and network capacity.* OVPIT staff expected that IU's campus network would be able to handle any traffic needs of online education since most users did not live on campus and because daily traffic typically peaked late at night, when most users were streaming HD videos from their dorm rooms. Tests were run on bandwidth consumption of services like Zoom versus Netflix and Amazon Prime video, and staff determined that even if all on-campus students used Zoom simultaneously, it would not match the bandwidth consumed by current video streaming platforms. Instead of the campus network, emphasis shifted to IU's VPN capacity. Because such a large percentage of students, faculty, and staff do not live on campus (>90% statewide), IT staff were concerned about the resources that could only be accessed from on-campus internet protocol (IP) addresses (file servers, web servers, library journal articles, etc.). IU's VPN was licensed for 4,000 simultaneous users and had a capacity of 10 gigabits per second. Within its contract, it could increase to 25,000 users for up to 56 days with no added cost. Prepandemic, the university was seeing peaks of 2,500 users and 500 megabits per second. Additional users could be added by purchase order to IU's vendor, but adding bandwidth would require equipment.

- *Commercial ISP capacity.* IU's IT leaders discussed middle and last-mile capacity with the commercial internet service providers (ISPs) in the areas where IU has campuses. Because the university would be dependent on commercial providers to carry traffic from their homes to the university data center via the VPN, it was critical that commercial

ISPs, especially in smaller towns like Bloomington, Kokomo, and Richmond, Indiana, would be able to handle the increase in traffic. The university received assurances that the commercial ISPs serving the areas around its campuses would have ample capacity.

- *Availability of hardware.* China, Japan, and Korea all began lockdowns before the United States, which started affecting supply chains and PC shipments as early as January 2020. Shipments to IU were delayed by as much as 6 to 8 weeks starting in February. In February 2020, OVPIT stopped decommissioning any functioning PC hardware that was life-cycle replaced in case such PCs were needed for staff to work remotely, or in case parts could be used to repair disabled PCs. IU's frontline support center and contact center staff had never previously worked from home. Many did not have the hardware to facilitate this at their homes. PCs and peripherals had to be procured in a time when hardware was difficult to come by. Some of the systems they accessed also required VPN use.

- *Internet access in remote areas.* The counties surrounding Bloomington in southern Indiana are quite rural. Many homes lack access to terrestrial internet, at any cost, and many lack cell reception as well. To accommodate this population of faculty, staff, and students, OVPIT acquired hundreds of 4G mobile hot spots to help staff work remotely. For those who could not use a cellular hot spot, IT staff set up parking-lot hot spots to allow users to sit in the safety of their cars and do their work, conduct e-learning, or otherwise connect.

- *Dependence on critical systems and cloud infrastructure*. Systems that would prove pivotal for online education, such as Zoom videoconferencing, the Canvas learning management system, and Kaltura video storage, were evaluated to ensure they could handle an increase in load. In each case, alternative products within IU's portfolio were identified.

- *Ability to handle the influx of questions related to the move to online.* Support and contact center staff were outfitted to work from home. While these staff were skilled at directing calls and troubleshooting problems, IU's campus teaching and learning center staff were the foremost experts in proper pedagogy and methods for online instruction. In the lead-up to the move to online instruction, the campus teaching and learning centers developed extensive documentation[1] and held webinars with thousands of faculty to help prepare them for online education.

Having a functional VPN would be critically important for this move to remote work, especially for IT staff who depended on systems that would require IP addresses in the VPN range to do their work. Removing these restrictions could pose significant security risks, but the hardware limits on VPN traffic speeds and CPU usage could also potentially become a chokepoint if too many users were to try to use the VPN for all their traffic. If usage were to increase, something

[1] keepteaching.iu.edu

would be needed to ensure the VPN would be there for the staff who needed it but would not get bogged down carrying unnecessary traffic.

Once it became clear the pandemic would increase demand for VPN use, we began weighing the cost of expanding the service versus the implications of capping demand. Expansion would mean a substantial increase in the costs of licensing and hardware. For every 5,000 users added, IU would have incurred costs of at least $50,000 per year for the needed virtual machine and user licenses. In addition, unforeseen network traffic patterns within the core network could have developed that may have resulted in additional expenses in reconfiguring network paths to support the VPN service. Because of the difficulty of obtaining appliance-based hardware early on in the pandemic, we would have been forced to use virtual machines to increase capacity and performance, an approach whose efficacy is not well known.

On the other hand, we wanted to ensure sensitive data and systems remained protected. We also wanted to be sure some excess VPN capacity was always available in case of an emergency, such as a business-interrupting event that would trigger our disaster recovery plans. Such an event might require teams to assemble and to perform emergency work virtually. This type of critical work is often sensitive and involves limited-access systems, and it therefore requires VPN use.

Ultimately, Indiana University decided to take a tailored, risk-based approach to VPN usage:

- *Users need only use VPNs when the service can't otherwise be accessed from outside IU.* This provides a layer of additional authentication for those services. All publicly accessible, enterprise IU websites are still protected by transport layer security (the encryption signified by "https" and the corresponding padlock that appears in your browser), and using VPN would be double-encrypting these sessions. By advising users in this way rather than encouraging a blanket approach of always using VPN, we intended to dramatically decrease demand, freeing it up for critical use.

- *Split tunneling is enabled.* As explained above, split tunneling keeps the home-to-cloud and any personal traffic from transiting our VPN and network. The VPN is relieved of all those personal Zoom calls, for example.

5. Communicating about appropriate VPN use

In the lead-up to the move to online instruction, university leadership sent a flurry of messages to users, outlining best practices on everything from ergonomics in the workspace to managing stress. One message from a non-IT campus leader included tips for staying safe online and suggested users make use of the VPN. That day, VPN use set a new record, and it never truly returned to prepandemic levels thereafter. IT had been very cautious about referencing the VPN in its emails to users so as to avoid drawing further attention to it; even using the phrase "Don't use the VPN" might lead to increased awareness and unnecessary use.

Instead, after split tunneling was implemented, OVPIT staff communicated with IT professionals throughout the university, as they would be the ones who would be in most need of the dedicated

VPN tunnels to access services. OVPIT staff also developed guidance for alternatives to the VPN.

Rather than use the VPN for accessing journal articles that were restricted by IP address, IT staff recommended using the library's proxy server, which would allow users the same access they had before. Students and scholars who were in countries that filter search results were encouraged—so long as they abided by national laws—to use IU's Citrix virtual applications and desktops, which would allow them to search the web as if they were in the United States. Finally, faculty and staff who had desktop PCs in their offices were encouraged to use remote desktop protocol if they needed access to on-campus file servers or to other services they had previously used in their offices.

To accompany the rollout of split tunneling, knowledge base documentation was developed on split tunneling[2] as well as on how to access resources from international locations.[3] Support staff were trained on the limitations of split tunneling and on alternatives so they could assist users who called for help.

6. Impact of this decision over the past 8 months

Thus far IU has observed no ill effects from our VPN "diet." We are not aware of any security incidents having occurred that VPN use would have prevented. Even after implementing split tunneling and our communications efforts, we have sustained a large increase in VPN usage. Prior to the pandemic and split tunneling, we typically saw an average of 1,500 users during a regular class day. That number immediately spiked to over 7,000 when everyone was sent home—before classes restarted. Once classes resumed and split tunneling was enabled, concurrent user peaks were around 6,000 until classes ended in the spring. Through the fall 2020 semester, peak concurrent usage has been around 5,000 users for days when classes are in session. Even with split tunneling enabled, bandwidth usage for the IU VPN has nearly tripled from prepandemic levels and has remained constant since. On the positive side, despite the increase in usage, we have not had to increase licensing or capacity.

To conclude, the potential resource issue IU faced at the beginning of the pandemic presented an opportunity to evaluate our risk calculus and to take a more efficient approach. In general, many risk analyses are based on hunches and incomplete knowledge, yet they are never fine-tuned as new knowledge is gained. In this case, IU was forced to reconsider the risks of reduced VPN usage and split tunneling and found them to be quite acceptable given the alternatives of fewer protected resources, less flexibility during emergencies, and insurmountable costs.

---

[2] https://kb.iu.edu/d/bexw

[3] https://kb.iu.edu/d/bgkg