code-for-a-living MARCH 13, 2020

Scaling your VPN overnight

We're 100% remote, as of Monday. And one of the critical tools that helps us work securely is our VPN. This article covers how we made our decision and best practices to follow.

Ben Popper
Director of Content

Starting on Monday of this week, Stack Overflow as a company went 100% remote, meaning all of our employees are now working from home. We put together tips from our staff about how to make remote work efficient, enjoyable, and sustainable.

One of the critical tools for enabling robust remote work in the software industry is a good virtual private network—VPN for short. Normally, when you work from outside of the office, data sent from your computer travels over the same public network as data from a consumer service, like a video streaming platform, online game, or shopping site. A VPN creates what's known as a tunnel: an encrypted link between your device and your work network, allowing your data to move in a secure manner, as if you were on a wired connection at your office.

With the current health crisis created by COVID-19, many countries and companies are asking people to work from home. This has created a sudden and massive surge in the number of employees working remotely each day. For many companies, their VPN infrastructure was not built to handle the entire organization working remotely and the need to scale quickly can prove challenging. So we sat down with some of the technical experts at Stack Overflow who built our VPN network to get their advice on pitfalls to avoid and best practices to follow.

"Over the years, we've used numerous vendors for our VPN system," says Brian Artschwager, the internal support engineer who leads up work on Stack Overflow's network. "One thing we ran into a lot was issues with dependability. Developers would be uploading a large file, the connection would drop, and they would have to start all over again."

Why we chose open source

In 2019 Stack Overflow switched to OpenVPN, an open source system written in C that was originally authored by James Yohan and released in 2001. "A lot of people, especially outside IT, still sometimes hesitate when it comes to open source, because there is a notion that it might somehow be less secure," says Artschwager. "But when a project has a deep history and a large group of people actively contributing to it, the reality is that it's likely to be the most robust and up to date software available."

There are a number of features that make OpenVPN the obvious choice for us. Since switching, dropped connections have become very rare. The service works well across a wide variety of operating systems and device types. Critically for Stack Overflow, it's SOC2 compliant, offers two-factor authentication, and as a result is approved for use when dealing with work for our enterprise level clients.

Don't mix business and pleasure

If your company is about to set up its first VPN or needs to dramatically scale up the number of users working through a VPN, Artschwager recommends going with a "split tunnel" approach. When using a VPN, data from a user appears to be coming from a specific, pre-set IP address. That is why VPNs are sometimes used to avoid geographic restrictions on internet traffic. A user with a VPN can communicate with a server and make it appear as if they are based in whatever region or country the VPN server exists within.

"We have developers in other countries and other states and they are connecting directly into our data center. The software on the user's computer gets an internal IP address that's in the same network or subnet as if it were a client on that physical network," says Artschwager. "The tunnel that you're generating is actually encapsulated and encrypted. Your traffic looks like one big encrypted stream of data, but on the other end of the connection it's just like you're directly connected."

With a split tunnel approach, only sensitive, work-related data is sent through the secure VPN tunnel to your work network. If you're at home watching cat videos on YouTube, that data will travel over your ordinary network. This can significantly reduce the load being put on your work's VPN servers and systems, ensuring everything stays up and running with minimal latency. "I know that we have developers that have gigabit internet connections. We don't want all of their traffic going to the data centers because it's not relevant for us and it just takes up bandwidth on our internet circuits. We have hundreds of employees using five

VPN servers in different locations and see barely any traffic because the only things that go over the connection are traffic that is destined for our internal systems."

Build extra capacity into your system

Over the year, Artschwager and his colleagues found that whether it's a hardware constraint or a licensing constraint, there's always an implied limit of how many people can connect to the same VPN. OpenVPN offers us thousands of connections and gigabytes of traffic.

We did have to buy "concurrently connected device" licenses for OpenVPN, but luckily we bought twice as many as we had users. That means folks working remotely now have options if they need to be on a laptop, tablet, and phone. "I'm reading reddit's /r/sysadmin/ subreddit and seeing the conversations in my peer group. People are talking about how they aren't sure how they are going to take a thousand people completely remote. Their VPN was only meant to support a few hundred people at once because it was built for remote sales people, for example, or their people at conferences. So far we haven't had that problem because we spec'd it for twice as many people as we had at the time."

Avoid routing through local offices

The majority of our VPN endpoints are actually in the data center, not regional offices, which frees up bandwidth for our employees. "Our data centers have access to really high bandwidth connections. By comparison, small regional offices or folks who work out of co-working spaces may be sharing internet access on a low throughput connection with dozens of employees or even other companies."

When considering how to build out your VPN, take stock of the data centers your company has access to, and try to find ways to maximize the throughput to locations with powerful, high bandwidth connections. Most data centers plan their operations around potential disruptions, building redundancy into their power and cooling systems, and will offer commitments to their customers to keep their technology operations running around the clock, so your VPN connection has less of a chance of going down for extended periods.

A checklist to help as you work to scale

Working remotely should be as secure as working in the office. If your organization is suddenly finding itself in need of a new or upgraded VPN solution, you'll need consider a few things:

- **Bandwidth:** Bandwidth utilization will increase with each additional client and residential internet speeds are constantly increasing. Users expect a fast connection and don't differentiate between what comes from the VPN connection and the public internet, so make sure your VPN solution can accommodate everyone's traffic.

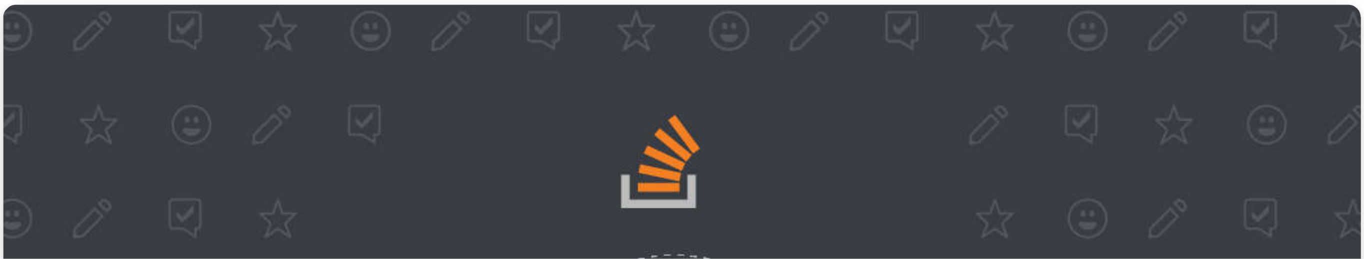
- **Stability:** Remote users depend on the connection and it should be as stable as being in the office. We performed 24 hour stress tests when choosing a vendor—we recommend everyone do the same.
- **Price per user:** Licensing can be different for each vendor. But generally the more licenses, the lower the price. This provides room for growth should user count increase. With employees potentially having multiple devices, user count may be more than you expect.
- **Security:** Remote users will be connecting from unsecured internet connections. Strong encryption is needed to secure the traffic to and from your corporate network. Multifactor authentication for your VPN can prevent unauthorized connections.

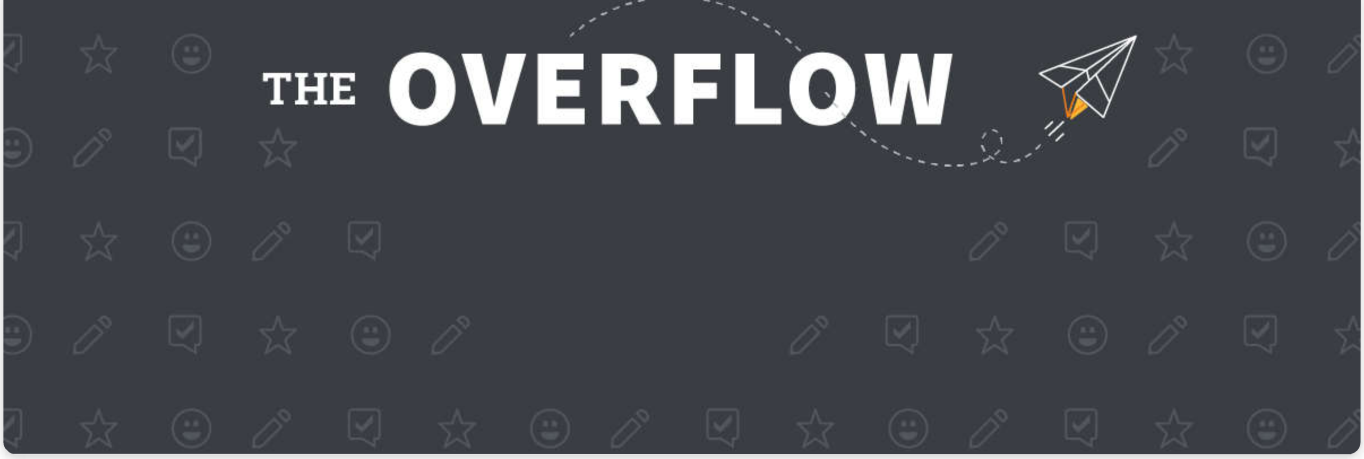
If you're looking to do further research, check out our questions on the tags openvpn and vpn. You can also leave a question in the comments—please keep it respectful and on topic—and we'll try to find time to answer them over the coming weeks.

Tags: announcements, stackoverflow, vpn

The Stack Overflow Podcast is a weekly conversation about working in software development, learning to code, and the art and culture of computer programming.

Related



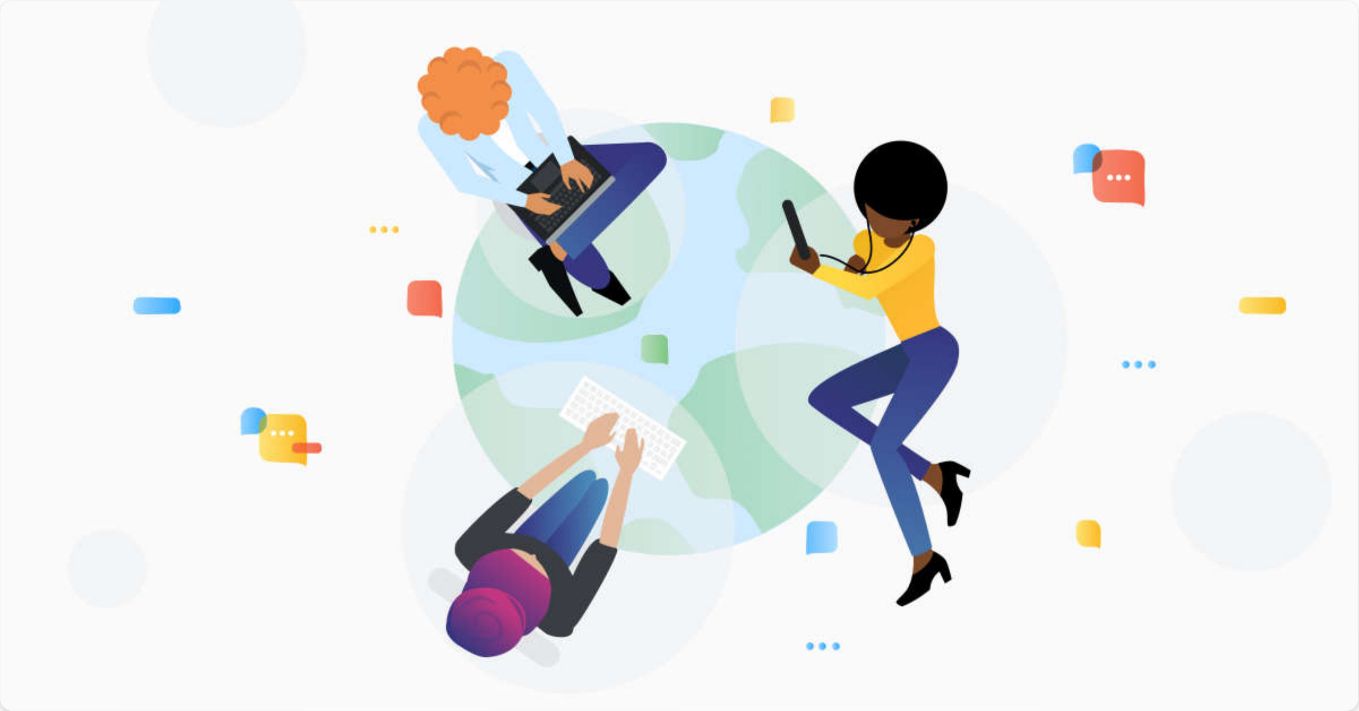


newsletter MARCH 20, 2020

The Overflow #13: The History of the URL

March 2020 Welcome to ISSUE #13 of The Overflow, a newsletter by developers, for developers, written and curated by the Stack Overflow team and Cassidy Williams of React Training. You can read more about it here. In this week's newsletter: how to stay sane while working remotely, the perils of 100% CPU load, and what's…

Ryan Donovan



promotion MARCH 19, 2020

Coming together as a community to connect

Stack Overflow is a community at our center. And communities come together in times of need. Our normal work routines have been disrupted and may continue to change for a while. We're all still defining the new "business as usual." We're all trying to figure out how to maintain team collaboration when lines of communication…

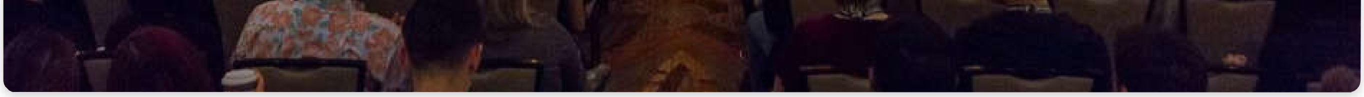
Lori Colston
Sr. Product Marketing Manager

talent APRIL 21, 2020

Why you should consider continuous remote options for your engineering team.

With the new situation, many people are adjusting to working remotely. While right now your team might be de facto remote, there is also the case to be made for seeing this as an opportunity to consider a remote or hybrid team as a lasting option. Allowing developers to work from wherever they're located is…

Medi Madelen Gwosdz
Content Strategist



talent DECEMBER 20, 2019

Making Remote Work at Stack Overflow – Interview Ilana Yitzhaki, Senior Manager, Employee Experience

Ilana Yitzhaki talks about how to create a great experience for employees in three Stack Overflow offices and remote Stackers across 14 countries. What does your current organizational setup look like and in which units do you work remotely?

Medi Madelen Gwosdz
Content Strategist

8 Comments

bob 14 Mar 20 at 12:30

you should try out wiregaurd

Reply

Roddy 15 Mar 20 at 12:59

There's a key thing you didn't mention: you absolutely should test your VPN at-scale *before* you need it. My company too routes its VPN endpoints to data centers, but we tested this week to see if they could support all 11,000 US employees working remotely. (Spoiler alert: they couldn't, but just barely.) Given that amount of lead time, we were able to address the issue ahead of being asked to be full-remote "for real" starting Monday.

Reply

Ross 17 Mar 20 at 11:35

Roddy, what did you use to load test your VPN? And what VPN vendor are you using? Thanks.

Reply

Pal 16 Mar 20 at 9:28

Use ZPA from Zscaler. It auto scales

Reply

Jonathan 27 Mar 20 at 3:55

Definitely Zscaler. A large amount of customers are coming to us because of COVID-19 and said their traditional VPN couldn't handle all of their employees working from home securely, with performance that scales. With Zscaler's ZPA connectors each has 500 Mbps throughput, and adding more connectors to accommodate additional user traffic is super easy.

Reply

Jonathan 27 Mar 20 at 4:00

Also, it's worth noting that Zscaler's technology is drastically different than a traditional network-to-network VPN, and focuses on ZTNA principals – i.e. Zero-Trust, user-to-application security. Our users are never placed on the network and our connectors are not internet facing which reduces attack surface area immensely. Look at all the VPN vulnerabilities that continue to take advantage of internet-facing VPN's, with 2019 very bad in particular, and the attacks aren't going to be stopping anytime soon…

Reply

Thales+Pereira 17 Mar 20 at 8:58

"But when a project has a deep history and a large group of people actively contributing to it, the reality is that it's likely to be the most robust and up to date software available." -> Is that really so? Linux had some critical bugs take around four years or more to be fixed.

Reply

Aron Pacey 12 May 20 at 8:14

I think bandwidth and security are the two key parameters while choosing a vpn from customer perspective. I have seen free vpn users complaining about internet speed issues due to limited bandwidth.

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

STACK OVERFLOW

- Questions
- Jobs
- Developer Jobs Directory
- Salary Calculator

PRODUCTS

- Teams
- Talent
- Advertising
- Enterprise

COMPANY

- About
- Press
- Work Here
- Legal
- Privacy Policy
- Contact Us

CHANNELS

- Podcast
- Newsletter
- Facebook
- Twitter
- LinkedIn
- Instagram