



**Ryan Gallagher** @rj\_gallagher Sat Sep 12 14:37:22 +0000 2020

A few people have asked me for more technical details about what U.S. company @Sandvine is doing in Belarus to help the country censor the internet. So here's a thread with some new insights on that:

Sandvine's technology was used to help shut down the internet in Belarus through several days in August, during & immediately after the disputed re-election of President Alexander Lukashenko, who is known as Europe's last dictator.

<https://t.co/Qt99aFr3Po>

The technology prevented people in Belarus from accessing social media websites such as Facebook & Twitter, messaging apps such as WhatsApp & Telegram, & international news websites.

Sandvine provided Belarus with its "Policy Traffic Switch" product, according to documents I've seen. It's a kind of "deep packet inspection" equipment, which can be used to filter, manage, & block, internet traffic. They look like this:

<https://t.co/yK3SA7GbMO>



You can find more information & technical details about the "Policy Traffic Switch" on Sandvine's website:

<https://t.co/HpkVzqzJ5R> (pdf)

The technology functions like a sort of probe, analyzing masses of internet data as it flows across networks. It has been installed at two sites in Minsk, within data centers operated by Belarus's government-controlled Network Traffic Exchange Center, docs show.

All internet traffic passing in & out of Belarus goes through the Network Traffic Exchange Center, & a large portion of it is filtered through Sandvine's policy traffic switches.

In a internal conference call on Thursday, Sandvine's chief technology officer Alexander Haväng said the company's technology is currently filtering 40% of all traffic going in & out of Belarus.

Sandvine offers network operators the ability to block websites by category, such as drugs, news, alcohol, gaming, abortion, & computer hacking, as this image from a company doc shows: <https://t.co/ONnj5DjBnE>



Figure 8 - Offer Pre-Configured, Network-based Web Filtering Services

The equipment can also be customized, enabling the network operator to add their own blacklists. In Belarus, that is what happened: the country added its own blacklists, & blocked thousands of sites, including Twitter, Facebook, CNN, BBC, & apps like WhatsApp, Viber & Telegram.

Some countries use the tech to block websites hosting child abuse images & pirated movies. But in the hands of a dictator it can be used for broad nationwide censorship, for example to stop people reading news stories revealing government corruption & abuse.

"You can sell a scalpel to a surgeon & someone else can use it to slash throats," said one employee of Sandvine, analogising the dual-use nature of the technology. "We sell the tech to places it can be misused. There's very little we can do once it's out the company's hands."

Network operators can block websites by adding lists of websites to the system & choosing to blacklist certain IP Classless Inter-Domain Routing blocks. The system can also block SSL encrypted websites through SSL Server Name Indication, according to Sandvine employees.

Sandvine says its systems have the capacity to stop people using censorship circumvention tools, like VPNs. It also claims it can block @PsiphonInc's anti-censorship tech, sources told me, though this is a "feature" that its customers have to pay for, according to employees.

In Belarus, some VPNs were blocked, but Psiphon was not, & it was widely used by Belarusians to circumvent the censorship, as I previously reported: <https://t.co/0U82YMjVSu> <https://t.co/nmFdvIJ11H>

By August 11, Toronto-based Psiphon Inc. had recorded more than 1.7 million unique users in Belarus, equal to nearly a fifth of the country's total population. Days earlier, the number of Psiphon users in Belarus had been a few thousand, according to the company. The internet disruption in the country - and people's sudden adoption of Psiphon to combat it - was comparable with previous incidents that have occurred in countries including Syria and Ethiopia, according to Michael Hull, president of Psiphon. (In those instances, it's not clear which vendors provided the Syrian and Ethiopian governments with equipment for the alleged internet shutdowns.)

Since August, amid ongoing protests in Belarus, Sandvine's technology has intermittently been deployed in the country to block access to VPNs & particular websites, including encrypted email provider Protonmail, & dozens of opposition political websites.

The company declined to comment. But told employees on Thursday it didn't consider blocking access to websites a human rights violation & didn't want to play "world police" by telling countries what they could & could not block. <https://t.co/D1fE6oJT6K>

"We don't want to play world police," he said. "We believe that each sovereign country should be allowed to set their own policy on what is allowed and what is not allowed in that country."

The revelations about Sandvine have prompted criticism from U.S. senators, a human-rights organization & Belarusians now living in the U.S., & have also ignited internal protests within Sandvine: <https://t.co/Qt99aFr3Po>