July 2020 ♦ Issue 7

Solutions

INSIDE THIS ISSUE

SSL VPN Reporting

Does 2020 seem like some dastardly science fiction movie, come to life? The pandemic has caused every business to re-engineer operational processes, and many organizations have safeguarded their workforce by instituting remote work-at-home capabilities by using a SSL VPN device. SSL VPN is a type of virtual private network solution which enables users to securely access servers that host web pages, applications, and other types of commonly used resources via an encrypted connection. A SonicWall SSL VPN device can greatly enhance Business Continuity Recovery processes. Moreover, this technology has enabled financial institutions to allow workers to perform job responsibilities away from the office seamlessly. But that has led to questions:

⇒ Which employees are actually working (or at least accessing the network?)
⇒ Who else is trying to access our systems?
⇒ When is peak time for remote access?

Deploying a VPN alone does not guarantee smooth IT operations. There are significant risks when transmitting data and it is important to know what activity is going on, on the network. To mitigate those risks and answer those above questions, organizations may want to keep track of who is doing what by keeping tabs on the number of active VPN sessions and measure the VPN session duration by using SSL VPN Reporting.

"SSL VPN Reporting is an important tool which provides detailed statistics on VPN usage."

SSL VPN Reporting is an important tool which provides detailed statistics on VPN usage. The report can point out discrepancies such as top failed VPN users which will be very helpful when trying to decipher if somebody is trying to compromise your VPN network.

AaSys®
Solutions are our Business

Continued on page 2

Repeated or abnormal failed connections would require a closer look. It lets you see if the VPN connection was terminated due to an auto-logout, a normal user logout, or any other reason as it might result in a possible attack. AaSys Group can help organizations understand the role remote access plays within their environment by configuring reporting software that provides a view of remote access activity. These reports can enlighten financial institutions to user behaviors and serve to highlight unintended activities.

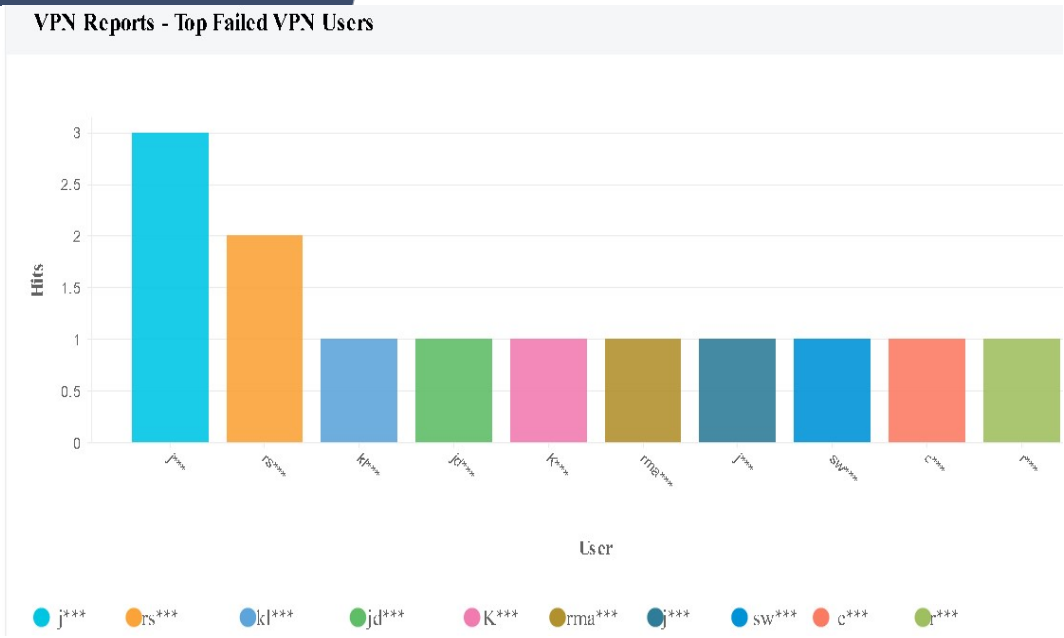


Image of AaSys Sample VPN Report-Top Failed VPN Users

Reporting will include insights such as:

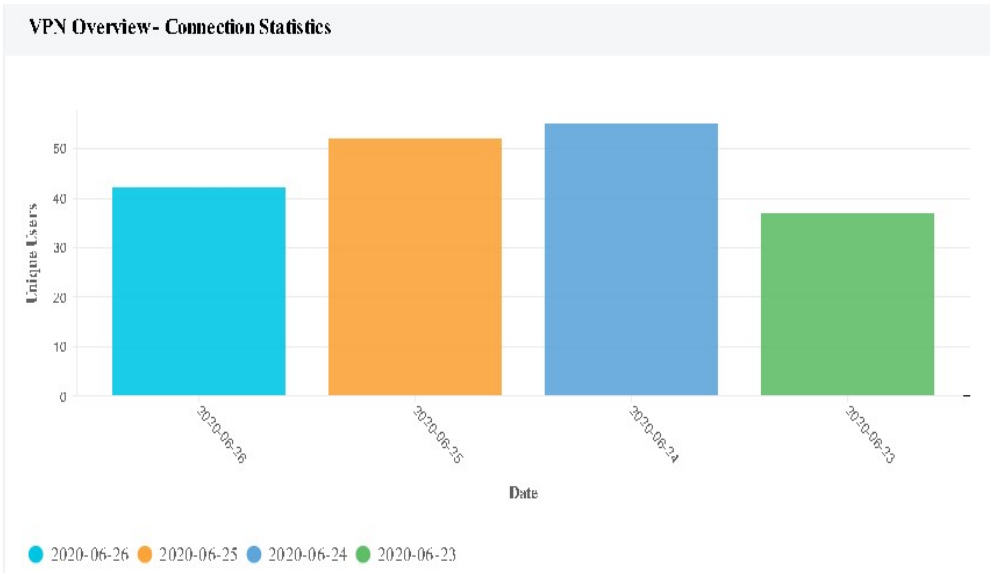
- **Remote Access Power Users (noted by total time of use of VPN)**
- **Total Usage of VPN by All Users**
- **Failed VPN Logins (This information can reveal the need for targeted training for remote users. Additionally, this report can uncover possible illicit surveillance)**
- **A log depicting every connection and disconnect for the month, along with the length of time for each connection, will be provided**

It is fair to say that over the next several months remote working is set to increase. It is important for organizations to adapt to the changes and to provide staff with secure VPN access to the applications and resources they need to do their jobs effectively, from wherever they may be. But it is equally important to ensure that security is also at the forefront.

Continued on page 3

According to the June 2020 Interagency Examiner Guidance (Assessing Safety and Soundness Considering the Effect of the COVID-19 Pandemic on Institutions), we know that examiners anticipate heightened cybersecurity risks. Fraud and cybersecurity controls to manage this risk are required and the documentation instructs examiners to review these controls. Reporting on remote usage is one such control.

The onslaught of the pandemic was sudden, causing everyone to scramble for solutions. Proper vetting of solutions might not have been as robust as usual. If your institution rolled out remote access for the first time, were you able to complete a risk assessment? In our haste to deploy technology, many of us found ourselves prioritizing tasks, and security may have taken a backseat.



Date	Unique Users	TotalCount
2020-06-26	42	53
2020-06-25	52	145
2020-06-24	55	150
2020-06-23	37	49

Image of AaSys Sample VPN Report-Connection Statistics

As the dust is settling, now is the time to review our controls. Conducting a cyber risk assessment is also advisable. This exercise will review all of your controls, including remote access. SSL VPN Reporting is also important to provide immediate answers to VPN usage questions posed by regulators or auditors. Reports can be generated daily, weekly, or monthly. Contact your Account Executive today to learn more about how SSL VPN Reporting can help your organization remain productive while keeping networks secure during the COVID-19 pandemic.

Sources:
https://www.sonicwall.com/products/remote-access/

5 Reasons to Keep Your Device Software in Compliance

At the end of March, there was a mad rush to get laptops and other portable devices into the hands of employees as quickly as possible due to the coronavirus pandemic. Device usage increased exponentially. But with that increase usage also came many security and IT challenges. One of those challenges are ensuring devices are up to date with the latest patches and software updates. A study published by Absolute showed that since the uptick in device usage, at least 1 in 4 devices have critical security apps that are out of compliance. On average, Microsoft Windows 10 devices were 78 days behind on patching and 8 out of 10 Windows devices were using versions more than one year old. Keeping your device software in compliance was always critical under normal circumstances but even more so now.

Software updates are important to your digital safety and overall cyber security. The sooner updates are deployed, the sooner you can feel confident your device is more secure, thus keeping the overall network of your organization secure as well.

Here are five reasons why it's important to update your device software regularly:

1. ***Repairs security holes that have been discovered and fixes or removes computer bugs.*** If security gaps are left unchecked hackers can take advantage of this weakness by writing code to target the vulnerability.
2. ***Protects your data and operating systems and helps keep hackers at bay.*** When you consider how nearly everything is stored digitally, your documents suddenly seem far more at risk than ever before. Software updates protect your data from theft by cyber criminals who try to exploit gaps in software in order to compromise your device.
3. ***Adds new features to your devices and removes outdated ones.*** Developers are constantly looking to add new and improve features to make the end-user experience better.
4. ***Improves performance and stability of the applications on your device.*** Software speed is important and also the updates provides better compatibility with different devices or applications.
5. ***Increases productivity.*** Sometimes your device may run slower than usual if it is not operating on the latest and greatest update which can possibly lead to a delayed turn around time to complete important task.

If you can keep every device and every app in your organization updated, you'll not only remain in compliance but will keep your organization safe from cyber vulnerabilities and the overall performance of your employees will improve. It is important to implement policies and practices to keep your devices and software up to date at all times.

Sources:
https:https://www.businesswire.com/news/home/20200430005292/en/New-Absolute-Insights-Reveal-Increases-Enterprise-Education
//www.absolute.com/it/
https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html