Tips for Ensuring the Availability and Security of Remote Access

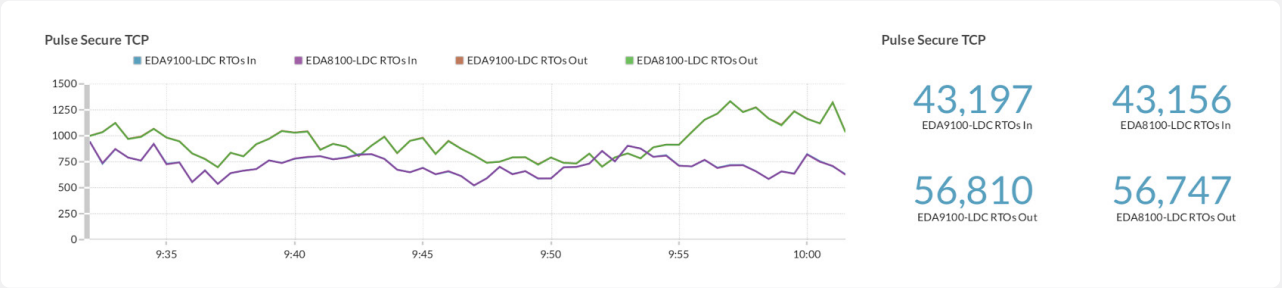
The COVID-19 pandemic is driving people to work from home and straining remote access infrastructure. Here are some considerations for IT and Security teams.

PERFORMANCE CONSIDERATIONS

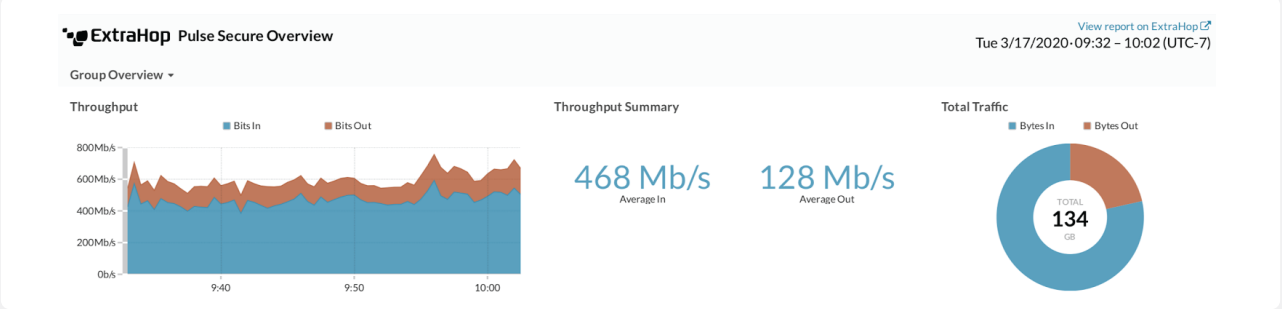
Dramatically increasing the number of people working from home is putting an incredible strain on remote access infrastructure as well as the Help Desk and IT teams handling the escalations.

Get ready for the "ghost in the machine" to manifest. Any tickets with "citrix" "vmware" or "cisco" will be routed to the remote access team who will be responsible for troubleshooting the issue. However, these systems are incredibly complex with many dependencies downstream—such as domain controllers and profile servers—and the remote access team may lack the visibility or expertise to diagnose the true problem.

In these cases, visibility across the entire delivery chain is critical to being able to triage and troubleshoot the issue. Keep in mind that many VPN issues will manifest at the transport protocol layer often in the form of retransmission timeouts and zero window measurements, while downstream issues with applications and resources will be apparent with Layer 7 analysis to identify errors and the associated conversations.



Measure utilization. You may lack adequate network bandwidth to handle the increased demand of remote users, so monitoring for bottlenecks at the gateway is critical to determine if a bigger pipe is needed. Additionally, while it's important to ensure remote users have access to applications and resources, you should not forget about measuring your organization's success (or failure) to provide that access. On the one hand, demonstrating how inadequate resources led to performance degradations, makes it easier to justify funding requests. On the other hand, if everything is going well, then measuring remote access utilization can help management understand the value that your team is providing to the business. Management may also be reassured by seeing that people are actually working while practicing self-distancing.



Part of a dashboard set up to monitor VPN activity by an ExtraHop customer.

SECURITY CONSIDERATIONS

Many remote workers have not been issued company laptops, and instead are now using unmanaged devices that lack adequate antivirus protections. In addition, the number of people working from home may force IT teams to loosen restrictions about what applications and data are accessible through the VPN.

Determine where people are remoting in from. IT organizations should pay attention to the geographic origin of external IPs connecting to their VPN concentrator or access gateway. Knowing where your users should be connecting from is very important, and one user connecting from two geographic locations will represent an actionable finding.

Are people using approved remote access tools? Many organizations have policies against using remote access tools such as TeamViewer, LogMeIn, and GoToMyPC. Enforcing these policies can go a long way toward securing sensitive applications and data, and looking at network communications is the fastest way to identify this type of activity.

Monitor Active Directory accounts. Look for excessive lock-outs, failed logins, and use of disabled accounts—all of which can indicate attackers have compromised a user device and are trying to gain access to more resources. Tracking service accounts for unusual behavior is a good idea, as is setting up "canary" accounts that act as a honeypot or tripwire catching attackers looking for more access in your network.

This is particularly critical given the large number of unmanaged personal devices now accessing the network. These unmanaged devices heighten the risk of stolen credentials, among other security implications.

People Are Still Your Greatest Asset

During this time, finding ways to work together, share information, and avoid finger pointing is critical. As noted in the "ghost in the machine" example, teams traditionally focused on one domain—whether end-user experience or security—may lack the visibility and expertise required to manage that under new conditions. Who knows? If we take this opportunity to reach out to our colleagues and get their input on how to solve the challenges we are facing together, then something good might come of this situation we find ourselves in.

LEARN MORE

If you'd like to learn more about ensuring the availability and security of remote access, visit www.extrahop.com

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101

info@extrahop.com
www.extrahop.com