SANS

Analyst Program

WhatWorks

What Works in Secure Remote Access: Giving Users Seamless and Secure Connectivity with Always-On Visibility and Management

Pulse Secure®

Introduction

Organizations have supported remote access for years now, but user complaints about complexity and performance remain high. Further, many VPN approaches cause breakage in ITs ability to manage and patch corporate laptops, as well as provide only limited visibility into endpoint security hygiene and status. The rapid movement to work from home to deal with the pandemic has magnified these deficiencies and accelerated the need for better approaches to remote access.

During this SANS WhatWorks webcast, Dan Connelly, IT Infrastructure Manager at Pittsburgh Plate Glass (PPG) will provide details on the selection and deployment of Pulse Secure's Secure Remote Access products. Connelly will also describe how to use these products to meet both business needs for full-time, work-from-home capabilities and IT operations needs for 24x7x365 ability to monitor and update configurations while maintaining high levels of security.

Join SANS Director of Emerging Security Trends John Pescatore and Dan Connelly to hear details on the selection, deployment and experience using Pulse Secure. The webcast will feature a discussion of lessons learned and best practices, as well as detail the metrics used to demonstrate the value of reliable, secure and always-on remote connectivity.

About the User

Dan Connelly is an IT Infrastructure Manager with responsibility for Internet-based services, including remote access for PPG, a Fortune 500 coatings company based in Pittsburgh, PA. Dan's team is responsible for the firewall services, load-balancing, global remote access services and secured internet access for 40,000 end users in more than 70 countries. When not securing network access, Dan enjoys bike-riding, playing guitar, making (and eating) pizza, and spending time with his family in Pittsburgh, PA.

About the Interviewer

John Pescatore joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Question

Tell us a little bit about your background, a little bit about PPG, and what your role is there.

Answer

PPG is a coatings manufacturer based in Pittsburgh. We are a 130-something years old and started as Pittsburgh Plate Glass in the late 1800s. We haven't made glass now in a while. Today it is paint, specialty coatings, industrial coatings and some fine chemicals.

I've been with PPG for 21 years, and I've been working with the telecom group in my role for about 12 years. I manage our internet-based services, which includes firewall, remote access, secure web gateway, some mobility solutions, load balancing and related services.

Question

Give us an idea of the scale—how many users there are, how many remote users, and so on.

Answer

PPG has about 40,000 employees, and about 35,000 of those have access to a computer and probably about 25,000 now have some remote access capabilities. They either have a company-provided laptop, or they can connect in with a personal computer and multifactor authentication. If they have their own PPG-issued laptop, then they most likely use Pulse Secure.

Question

What was the business problem that caused you to evaluate remote access approaches?

Answer

Remote access is not a new requirement, but we were a manual VPN shop for a long time. If the user had a laptop when they were at home and they needed corporate connectivity, they engaged their VPN. We were using Juniper, and so the user went to a URL and established an HTTP SSL VPN session.

That met the user need for connectivity, but we needed to make sure we could manage computers and not let them fall out of the domain. Many users would have both a desktop and a laptop, but they might not connect to their laptop for 90 days. By that time, that laptop would fall out of the domain, and it would cause a lot of problems. For IT people, you couldn't go after anything with an IP address. Everything had to be a fully qualified domain name. So it was very hard to do IP-related troubleshooting, traceroutes, pings, things like that. Some applications weren't fully qualified name aware or they used this modified virtual IP V6 stack, and some legacy applications didn't work.

We were urged to find a solution that would allow the machine itself to make a connection and not depend on the user to do that. As soon as the laptop hit the internet, we wanted it to automatically build the tunnel, without the user controlling that. We looked at Microsoft's Direct Access. On paper, it worked. It met the needs, so we deployed it.

However, we have eight data centers now with users all over the world. We try to route the users to the closest data center for whatever external services that we host for them. And in order to do this with Direct Access, we had to rely on Group Policy Objects [GPO] which, for us, created a whole bunch of challenges. What we discovered was that having a GPO approach meant if something happened to that policy, it affected all of the users all at the same time, which caused disruptions and confusion.

We also found that with Direct Access and some of the other solutions we tried, reliability and consistency weren't quite there. We would

have users sometimes in their home, coffee shop, or other places where they didn't have a strong Wi-Fi connection. They would drop off of the workstation tunnel, and it might take five minutes or more for them to connect. Since we have a split-brain DNS at PPG, we would have users that would connect to the VPN, cache a lot of internal PPG.com DNS entries and get disconnected. They would then cache external DNS entries, which would mess everything up when they reconnected. For a number of years, the most common help desk calls were related to our legacy remote access service.

The ability to do a split tunnel was also key for us. We use internet filtering, and if you're on the corporate network, we block streaming video. We block video, we block apps like Spotify and everything like that. But if you're on your home network, we don't care because that's bandwidth that's not consumed and shared by other users. To support today's environment, you need to be able to do that, and we had a lot of problems doing this with Direct Access.

Basically, we started looking for a solution that would be more transparent to the users, would allow us to have 24x7x365 management over remote assets while reducing those help desk calls.

The Pulse Secure automatic VPN was a stable product. We did an evaluation on it, and we liked it. We noticed right away that it solved the connectivity problems and worked across our split DNS environment. We had a lot of other products in-house with remote access capabilities, and we looked at those, too. We use Palo Alto [Networks] firewalls that have GlobalProtect enabled, and we tested that. We used [Citrix] NetScaler, which also has a VPN function; we looked at that.

But the Pulse Secure approach was clearly superior. We enabled it and eventually moved to it for production, and those help desk calls have largely gone away.

We don't have the persistent issues that we've seen before with some of the other solutions. We've been running successfully since the end of 2018.

Question

How long did it take you to go operational?

Answer

It was not a complex migration, but external factors slowed us down. There were a lot of changes that were happening. We were in the process of going from Windows 7 to Windows 10 and some organizational changes. It took a couple of months to get the initial upgrade rolling up and running, and then about four more months to reach the full 24,000 users. It all went very smoothly.

After we had been running successfully for a while, PPG acquired a company in Mexico. They were using Cisco AnyConnect, using old concentrators that were no longer being supported. We knew we had to get them onto a supported approach with minimal disruption to their ongoing operations. Zscaler has a reverse proxy product called Zscaler Private Access (ZPA) that we looked at but we needed the ability to do a bidirectional initiation of the tunnel, and ZPA was, at the time, just one directional. Once we learned that, we decided to go with Pulse.

The business side was worried about what to them was a brand-new solution, but since we had already demonstrated how well Pulse Secure worked on the corporate side, we got the OK and deployed that very quickly.

Question

Knowing what you know today, is there anything you'd do differently, any lessons learned you'd be able to pass on to our readers?

Answer

I would have looked for more of a hardware-based solution earlier on in the process and would have avoided using a server OS to do all the VPN tunneling. I think we had somewhere around 32 different Direct Access servers at one time to cover all of our users. With one or two of the Pulse Secure appliances, we can cover all of our population. The hardware approach was a much lighter footprint and made failover for redundancy much easier to be implemented.

Another thing we did that worked out really well was to go with a little bit of a larger box, even though it seemed, on paper, we enabled far too much capacity. We knew that there are times, when either we're doing data center maintenance or for any other reason, we want to move internet traffic from one location to another. We really wanted the ability to pick and choose where we brought users in and have the option to bypass one or multiple data centers at any time for this service.

The decision turned out to be beneficial regarding this COVID situation because we had some locations where we had a little bit better bandwidth into that location than others. So we had the flexibility to move the traffic around however we needed to do that. In 2009, Pittsburgh, where our headquarters is, was hosting the G8 economic conference and the city didn't want anybody in town that didn't need to be in town. So we had all of our Pittsburgh workforce working from home. We were really nervous at the time about the local remote access support that we had coming into our local data center. From that lesson we learned, if there's ever a global event—and it could be a weather event, an epidemic, a pandemic or anything—we really wanted to make sure that we could ramp up and support any number of users in any of our data center locations.

Question

How's the support been from Pulse Secure in helping you keep everything up and running and up-to-date?

Answer

The support has been very good for us.

After we deployed, we had a professional service engagement with a Pulse engineer that did an audit of our environment and double-checked everything. He's been a great support for us whenever we have something that's a little bit odd.

We haven't had any outages, and I think we have only had one RMA where we sent a device back, and it happened just to be a test device. The product quality and support is as good or better than any other vendor that we have today.

About Pulse Secure

Pulse Secure provides easy, comprehensive software-driven Secure Access solutions for people, devices, things and services that improve visibility, protection, and productivity for our customers. Our suites and SaaS platform uniquely integrate cloud, mobile, application and network access to enable hybrid IT in a Zero Trust world. Over 24,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely connect to applications and information across the data center and multi-cloud while ensuring business compliance.

About SANS WhatWorks

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned.